一生懸命にFSCP技術内容 &合格スムーズFSCP試験準備 |有難いFSCP復習時間Forescout Certified Professional Exam

多くのIT者がForescoutのFSCP認定試験を通してIT業界の中で良い就職機会を得たくて、生活水準も向上させたいです。でも多くの人が合格するために大量の時間とエネルギーをかかって、無駄になります。同等の効果は、JPNTestは君の貴重な時間とお金を節約するだけでなく１００％の合格率を保証いたします。もし弊社の商品が君にとっては何も役割にならなくて全額で返金いたいます。

Forescout FSCP 認定試験の出題範囲:

トピック	出題範囲
トピック 1	• ポリシー機能: 試験のこのセクションでは、ポリシー実装者と統合スペシャリストのスキルを測定し、依存関係、ルールの順序、適用トリガー、デバイス分類および動的属性との相互作用など、プラットフォーム内でのポリシーの動作をカバーします。
トピック 2	• プラグイン チューニング HPS: 試験のこのセクションでは、プラグイン開発者とエンドポイント統合エンジニアのスキルを測定し、ホスト プロパティ スキャナー (HPS) プラグインのチューニング (エンドポイントのプロファイル作成、スキャン ロジックの調整、例外の処理、適用のための正確なホスト属性収集の確保など) について扱います。
トピック 3	• FSCA トピックの概説：このセクションでは、ネットワークセキュリティエンジニアとシステム管理者のスキルを測定します。アーキテクチャ、資産の識別、初期導入時の考慮事項など、プラットフォームの基本的な概念を幅広く網羅しています。より高度な分野に進む前に、関連するベースライントピックに精通していることを確認します。| ポリシーのベストプラクティス：このセクションでは、セキュリティポリシーアーキテクトと運用管理者のスキルを測定します。堅牢なポリシーを効果的に設計および適用する方法を取り上げ、技術的な構成だけでなく、保守性、明確性、組織目標との整合性を重視します。
トピック 4	• プラグイン チューニング ユーザー ディレクトリ: 試験のこのセクションでは、ディレクトリ サービス インテグレーターと ID エンジニアのスキルを測定し、ユーザー ディレクトリと統合するプラグインのチューニング (構成、ディレクトリ属性のプラットフォーム ポリシーへのマッピング、パフォーマンスに関する考慮事項、セキュリティ上の影響など) をカバーします。
トピック 5	• 高度な製品トピックの証明書と ID 追跡: 試験のこのセクションでは、ID およびアクセス制御のスペシャリストとセキュリティ エンジニアのスキルを測定し、デジタル証明書の管理、PKI 統合、ID 追跡メカニズム、およびそれらがシステム内での適用と監査機能をどのようにサポートするかをカバーします。

トピック 6	• 高度なトラブルシューティング: 試験のこのセクションでは、運用リーダーと上級テクニカル サポート エンジニアのスキルを測定し、表面的な修正だけでなく、コンポーネントの相互作用、ポリシー適用の失敗、プラグインの誤動作、根本原因の分析と修正戦略を必要とするエンドツーエンドのワークフローにわたる複雑な問題の診断をカバーします。
トピック 7	• 高度な製品トピックのライセンス、拡張モジュール、冗長性: 試験のこのセクションでは、製品導入リーダーとソリューション エンジニアのスキルを測定し、ライセンス モデル、オプションのモジュールまたは拡張機能、高可用性または冗長性の構成、それらがアーキテクチャと運用の準備にどのように影響するかなどのトピックをカバーします。
トピック 8	• カスタマイズされたポリシーの例: 試験のこのセクションでは、セキュリティ アーキテクトとソリューション配信エンジニアのスキルを測定し、シナリオベースのポリシー設計と実装をカバーします。ビジネス ケースの要件を理解し、カスタマイズされたポリシー フレームワークを作成し、例外的なデバイスやワークフローに合わせて調整し、コンテキスト内でそれらのカスタマイズを文書化または検証する必要があります。
トピック 9	• プラグイン チューニング スイッチ: 試験のこのセクションでは、ネットワーク スイッチ エンジニアと NAC (ネットワーク アクセス制御) スペシャリストのスキルを測定します。スイッチ ポートの監視、レイヤー 2 • 3 の統合、ネットワーク インフラストラクチャ経由の ACL または VLAN の割り当てなどのスイッチ関連プラグインのチューニングと、それらのネットワーク資産を通じた可視性と制御の維持が対象となります。

>> FSCP技術内容 <<

FSCP試験準備 & FSCP復習時間

ForescoutのFSCPのオンラインサービスのスタディガイドを買いたかったら、JPNTestを買うのを薦めています。JPNTestは同じ作用がある多くのサイトでリーダーとしているサイトで、最も良い品質と最新のトレーニング資料を提供しています。弊社が提供したすべての勉強資料と他のトレーニング資料はコスト効率の良い製品で、サイトが一年間の無料更新サービスを提供します。ですから、弊社のトレーニング製品はあなたが試験に合格することを助けにならなかったら、全額で返金することを保証します。

Forescout Certified Professional Exam 認定 FSCP 試験問題 (Q21-Q26):

質問 # 21
If the condition of a sub-rule in your policy is looking for Windows Antivirus updates, how should the scope and main rule read?

- A. Scope "corporate range", filter by group "None", main rule "member of Group = Windows"
- B. Scope "corporate range", filter by group "windows managed", main rule "No conditions"
- C. Scope "all ips", filter by group blank, main rule member of group "Windows"
- D. Scope "all ips", filter by group "windows", main rule "No Conditions"
- E. Scope "threat exemptions", filter by group "windows managed", main rule "member of group = windows"

正解：B

解説：
Comprehensive and Detailed Explanation From Exact Extract of Forescout Platform Administration and Deployment:
According to the Forescout Administration Guide - Define Policy Scope documentation and Windows Update Compliance Template configuration, when the condition of a sub-rule is looking for Windows Antivirus updates, the scope and main rule should read: Scope "corporate range", filter by group "windows managed", main rule "No conditions".
Policy Scope Definition:
According to the policy scope documentation:
When defining the scope for a Windows Antivirus/Updates policy:
* Scope - Should be set to "corporate range" (endpoints within the corporate IP address range)
* Filter by group - Should filter by the "windows managed" group (Windows endpoints that are manageable)
* Main rule - Should have "No conditions" (meaning the policy applies to all endpoints matching the scope and group) Why "No conditions" for the Main Rule:

According to the Windows Update Compliance Template documentation:
The main rule is designed to be:
* Broad in scope - Applies to all eligible Windows managed endpoints
* Without specific conditions - Specific conditions are handled by sub-rules
* Efficient filtering - The scope and group filter do the initial endpoint selection The sub-rules then contain the specific conditions (e.g., "Windows Antivirus Update Date < 30 days ago") to evaluate each endpoint's compliance.
Policy Structure for Windows Updates:
According to the documentation:
text
Policy Scope: "Corporate Range"
Filter by Group: "windows managed"
Main Rule: "No Conditions"
Sub-rule 1: "Windows Antivirus Update Date > 30 days"
Action: Trigger update
Sub-rule 2: "Windows Antivirus Running = False"
Action: Start Antivirus Service
Sub-rule 3: "Windows Updates Missing = True"
Action: Initiate Windows Updates
"Windows Managed" Group:
According to the policy template documentation:
The "windows managed" group specifically includes:
* Windows endpoints that can be remotely managed
* Endpoints with proper connectivity to management services
* Systems with necessary admin accounts configured
* Machines capable of executing remote scripts and commands
Why Other Options Are Incorrect:
* A. Scope "all ips", filter by group blank, main rule member of group "Windows" - Too broad scope (includes non-Windows systems); "all ips" is inefficient
* B. Scope "corporate range", filter by group "None", main rule "member of Group = Windows" - Correct scope and filtering wrong (should filter by group, not in main rule)
* C. Scope "threat exemptions", filter by group "windows managed", main rule "member of group = windows" - Wrong scope (threat exemptions is for excluding systems); redundant main rule
* E. Scope "all ips", filter by group "windows", main rule "No Conditions" - Too broad initial scope; "all ips" is inefficient and includes non-corporate systems Recommended Policy Configuration:
According to the documentation:
For Windows Antivirus/Updates policies:
* Scope - Define as "corporate range" to limit to organizational endpoints
* Filter by Group - Set to "windows managed" to exclude non-manageable systems
* Main Rule - Set to "No conditions" for simplicity; let scope/group do the filtering
* Sub-rules - Define specific compliance conditions (e.g., patch level, antivirus status) This structure ensures:
* Efficient policy evaluation
* Only applicable Windows endpoints are assessed
* Manageable systems are prioritized
* Specific compliance checks occur in sub-rules
Referenced Documentation:
* Define Policy Scope documentation
* Windows Update Compliance Template v2
* Defining a Policy Main Rule

質問 # 22
When configuring a Send Email action to notify CounterACT administrators, how do you add endpoint specific host information to the message?

- A. Edit the "Message to Email Recipient" Field of the Send Email action Parameters tab, then click 'Tag" to add the desired property value.
- B. Create criteria in sub-rules to detect the desired specific host information. The "Send Email" action will send this information to the CounterACT administrator.
- C. Edit the Options > General > Mail settings and click "Tag" to add the desired property values.
- D. Edit the "Message to Email Recipient" Field of the Send Email action Parameters tab, then click 'Tag" to add the desired

keyword tag.
- E. It is not possible to add specific host information for detected endpoints.

正解：A

解説：
Comprehensive and Detailed Explanation From Exact Extract of Forescout Platform Administration and Deployment:
According to the Forescout Administration Guide - Send Email action documentation, to add endpoint- specific host information to a Send Email notification, you should "Edit the 'Message to Email Recipient' Field of the Send Email action Parameters tab, then click 'Tag' to add the desired property value".
Property Tags in Send Email Action:
According to the Property Tags documentation:
"Property tags insert endpoint values into condition or action fields, and are replaced by the actual endpoint property value when the field is evaluated." Property tags allow dynamic insertion of endpoint-specific data into email messages.
How to Add Property Tags to Email:
According to the documentation:
* Edit Send Email Action - Open the Send Email action configuration
* Navigate to Parameters Tab - Select the Parameters tab
* Edit Message Field - Edit the "Message to Email Recipient" field
* Click Tag Button - Select the "Tag" button/option
* Choose Property - Select the endpoint property to insert (e.g., IP address, OS, etc.)
* Confirm - The property tag is inserted into the message
Example Email Message with Property Tags:
According to the More Action Tools documentation:
text
Example message:
"Endpoint [IP.Address] with hostname [IP.Hostname]
has failed compliance check for operating system [OS]."
When evaluated:
"Endpoint 192.168.1.50 with hostname WORKPC-01
has failed compliance check for operating system Windows 10."
Available Properties for Tags:
According to the documentation:
Property tags can reference:
* IP Address
* MAC Address
* Hostname
* Operating System
* Device Function
* User information
* Custom endpoint properties
Why Other Options Are Incorrect:
* A. Create criteria in sub-rules - Sub-rules don't send email; they're for conditional logic
* C. Edit Options > General > Mail settings - This is for global email configuration, not message customization
* D. It is not possible - Incorrect; property tags specifically enable this functionality
* E. "Keyword tag" - The feature uses "property tags" or "tags," not "keyword tags" Referenced Documentation:
* Send Email action
* Property Tags
* More Action Tools - Property tags section

質問 # 23
How can a specific event detected by CounterACT (such as a P2P compliance violation event) be permanently recorded with a custom message for auditing purposes?

- A. Customize the message on the send syslog action
- B. Customize the message in the Reports Portal
- C. Configure a custom SNMP trap to be sent
- D. Increase the "Purge Inactivity Timeout" setting
- E. Customize the message in the syslog configuration in Options > Core Ext > Syslog

正解：A

解説：
Comprehensive and Detailed Explanation From Exact Extract of Forescout Platform Administration and Deployment:
According to the Forescout Administration Guide and Syslog Plugin Configuration Guide, specific events detected by CounterACT can be permanently recorded with a custom message for auditing purposes by customizing the message on the send syslog action.
Send Message to Syslog Action:
According to the official documentation:
"You can send customized messages to Syslog for specific endpoints using the Forescout eyeSight Send Message to Syslog action, either manually or based on policies." How to Configure Custom Messages:
According to the Syslog Plugin Configuration Guide:
* Create or Edit a Policy - Select a policy and edit the Main Rule section
* Add an Action - In the Actions section, select "Add"
* Select Send Message to Syslog - From the Audit folder, select "Send Message to Syslog"
* Customize the Message - Specify the custom message to send when the policy is triggered Custom Message Configuration:
According to the documentation:
When configuring the "Send Message to Syslog" action, you specify:
* Message to syslog - Type a custom message to send to the syslog server when the policy is triggered
* Message Identity - Free-text field for identifying the syslog message
* Syslog Server Address - The syslog server to receive the message
* Syslog Server Port - Typically port 514
* Syslog Server Protocol - TCP or UDP
* Syslog Facility - Message facility classification
* Syslog Priority - Severity level (e.g., Info)
Example Implementation for P2P Compliance Violation:
According to the configuration guide:
For a P2P compliance violation event, you would:
* Create a policy that detects P2P traffic violations
* Add a "Send Message to Syslog" action
* Customize the message to something like: "P2P VIOLATION: Endpoint [IP] detected unauthorized P2P application traffic"
* Configure the syslog server details
* When the condition is triggered, CounterACT sends the custom message to syslog for permanent auditing Permanent Recording:
According to the documentation:
The messages sent to syslog are:
* Permanently recorded on the syslog server
* Timestamped automatically by Forescout and/or the syslog server
* Available for audit trails and compliance reports
* Can be forwarded to SIEM systems like Splunk or EventTracker for further analysis Why Other Options Are Incorrect:
* B. Increase the "Purge Inactivity Timeout" setting - This relates to device timeout, not event recording or custom messages
* C. Customize the message in the Reports Portal - The Reports Portal displays reports but does not customize messages for syslog events
* D. Configure a custom SNMP trap - SNMP traps are for network device management, not for recording Forescout events
* E. Customize the message in the syslog configuration in Options > Core Ext > Syslog - While syslog configuration is done here, the actual custom messages are configured in the "Send Message to Syslog" action within policies Referenced Documentation:
* How-To Guide: ForeScout CounterAct to forward logs to EventTracker
* Audit Actions documentation
* How to Work with the Syslog Plugin
* Send Message to Syslog Action documentation

質問 # 24
Which of the following plugins assists in classification for computer endpoints? (Choose two)

- A. HPS Inspection Engine
- B. Switch
- C. Advanced Tools
- D. DNS Client
- E. Linux Plugin

正解：A、C

解説：
Comprehensive and Detailed Explanation From Exact Extract of Forescout Platform Administration and Deployment:
According to the Forescout Administration Guide and Base Modules documentation, the plugins that assist in classification for computer endpoints are HPS Inspection Engine (B) and Advanced Tools (D).
HPS Inspection Engine Classification:
According to the HPS Inspection Engine Configuration Guide:
"The HPS Inspection Engine powers CounterACT tools used for classifying endpoints. These tools include the classification engine that is part of HPS Inspection Engine, the Primary Classification, Asset Classification and Mobile Classification templates, the Classify actions, and Classification/Classification (Advanced) properties." The HPS Inspection Engine provides:
* Classification Engine - Determines the Network Function property
* Primary Classification Template - Classifies endpoints into categories
* Asset Classification Template - For asset-level classification
* Mobile Classification Template - For mobile device classification
* Multiple Classification Methods - Including NMAP, HTTP banner scanning, SMB analysis, passive TCP/IP fingerprinting
Advanced Tools Plugin Classification:
According to the Advanced Tools Plugin documentation:
"The Advanced Tools Plugin is used to classify endpoints based on characteristics such as operating system, hardware vendor, and application software." The Advanced Tools Plugin provides:
* Endpoint Classification - Based on OS, vendor, and applications
* Device Property Resolution - Resolves device characteristics
* Fingerprinting - Identifies endpoints based on behavioral patterns
Why Other Options Are Incorrect:
* A. Switch - The Switch Plugin manages network devices (switches) and provides VLAN/access control, not endpoint classification
* C. Linux Plugin - The Linux Plugin is a platform-specific module for managing Linux endpoints, not a general classification tool
* E. DNS Client - The DNS Client Plugin resolves DNS queries but does not assist with endpoint classification Classification Workflow:
According to the documentation:
When classifying computer endpoints, Forescout uses:
* HPS Inspection Engine - Primary classification tool analyzing:
* HTTP banners from web services
* SMB protocol information
* NMAP scans and service detection
* Passive TCP/IP fingerprinting
* Domain credentials analysis
* Advanced Tools Plugin - Secondary classification providing:
* Vendor/model information
* Application detection
* Operating system identification
* Hardware characteristics
Together, these plugins provide comprehensive endpoint classification for computer systems.
Classification Properties Resolved:
According to the Base Modules documentation:
The HPS Inspection Engine and Advanced Tools plugins resolve:
* Function (Workstation, Printer, Server, Router, etc.)
* Operating System (Windows, Linux, macOS, etc.)
* Vendor and Model information
* Network Function (specific device role)
* Application information
Referenced Documentation:
* CounterACT Endpoint Module HPS Inspection Engine Configuration Guide v10.8
* Forescout Platform Base Modules
* About the Forescout Advanced Tools Plugin

質問 # 25
What is the default recheck timer for a NAC policy?

- A. 8 hours
- B. 12 hours

- C. 4 hours
- D. 2 hours
- E. 24 hours

正解：A

解説：
Comprehensive and Detailed Explanation From Exact Extract of Forescout Platform Administration and Deployment:
According to the Forescout Administration Guide - Policy Main Rule Advanced Options, the default recheck timer for a NAC policy is 8 hours.
Default Policy Recheck Timer:
According to the official documentation:
"By default, both matched endpoints and unmatched endpoints are rechecked every eight hours, and on any admission event." This 8-hour default ensures that all endpoints are periodically re-evaluated against policy conditions, regardless of whether they currently match the policy.
Recheck Configuration:
According to the documentation:
When you configure a policy's main rule advanced options:
* Default Recheck Interval: 8 hours
* Customizable Range: Can be configured from 1 hour to infinite (no recheck)
* Applies to: All endpoints in the policy scope
Recheck Triggers:
According to the administration guide:
Policies recheck when:
* Recheck Timer Expires - Every 8 hours by default
* Admission Event - When specific network events occur
* SecureConnector Event - When SC status changes
Referenced Documentation:
* Forescout Platform Policy Main Rule Advanced Options
* Main Rule Advanced Options

質問 # 26
.....

お客様に自分に一番ふさわしいForescoutのFSCP試験の復習方式を提供するために、我々はForescoutのFSCPの資料の3つのバーションを提供します。PDF、オンライン版とソフト版です。あなたの試験準備にヘルプを提供するのは常にあります。すべてのバーションは無料のデモを提供します。そのほかに、どのバーションでも全面的で最新版のForescoutのFSCPの資料を提供します。

FSCP試験準備: https://www.jpntest.com/shiken/FSCP-mondaishu

- FSCP模擬試験問題集 □ FSCP赤本合格率 □ FSCP問題と解答 □ Open Webサイト⇒ www.shikenpass.com ⇐検索▹ FSCP ◃無料ダウンロードFSCP一発合格
- FSCP日本語復習赤本 □ FSCP学習範囲 □ FSCP日本語版受験参考書 □ ▸ www.goshiken.com ◂で使える無料オンライン版▹ FSCP ◃ の試験問題FSCP模擬試験問題集
- 効果的FSCP｜素晴らしいFSCP技術内容試験｜試験の準備方法Forescout Certified Professional Exam試験準備 □ □ www.passtest.jp □に移動し、{ FSCP }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FSCP専門試験
- FSCP模試エンジン □ FSCP受験対策 □ FSCP復習教材 □ ➠ www.goshiken.com □サイトにて➥ FSCP □問題集を無料で使おうFSCP教育資料
- FSCP試験、FSCP勉強資料バージョン、Forescout Certified Professional Exam試験日程 □ 【 www.it-passports.com 】を入力して【 FSCP 】を検索し、無料でダウンロードしてくださいFSCP赤本合格率
- 更新するFSCP技術内容 - 合格スムーズFSCP試験準備 | 大人気FSCP復習時間 □ 【 www.goshiken.com 】サイトにて最新➡ FSCP □□□問題集をダウンロードFSCP模試エンジン
- 効果的FSCP｜素晴らしいFSCP技術内容試験｜試験の準備方法Forescout Certified Professional Exam試験準備 □ ▹ www.jptestking.com ◃で[FSCP]を検索して、無料で簡単にダウンロードできますFSCP対応問題集
- 一番優秀なForescout FSCP技術内容 - 合格スムーズFSCP試験準備 | 最高のFSCP復習時間 □ ➠ www.goshiken.com □で使える無料オンライン版▹ FSCP ◃ の試験問題FSCP的中合格問題集
- FSCP合格体験談 □ FSCP受験対策 □ FSCP日本語版受験参考書 □ ➠ jp.fast2test.com □に移動し、《 FSCP 》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FSCP専門試験

- Forescout FSCP技術内容: Forescout Certified Professional Exam - GoShiken 最終更新ダウンロード □（ FSCP ）の試験問題は □ www.goshiken.com □で無料配信中FSCP練習問題集
- オールインワンタイプの FSCP 参考書＆問題集 □【 www.it-passports.com 】に移動し、「 FSCP 」を検索して無料でダウンロードしてくださいFSCP合格体験談
- 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, whatoplay.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, mecabricks.com, bbs.t-firefly.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, www.stes.tyc.edu.tw, Disposable vapes