

Types of Real Forescout FSCP Exam Questions



If you would like to use all kinds of electronic devices to prepare for the FSCP exam, with the online app version of our FSCP study materials, you can just feel free to practice the questions in our FSCP training materials no matter you are using your mobile phone, personal computer, or tablet PC. In addition, another strong point of the online app version is that it is convenient for you to use even though you are in offline environment. In other words, you can prepare for your FSCP Exam with under the guidance of our FSCP training materials anywhere at any time.

We hold on to inflexible will power to offer help both providing the high-rank FSCP exam guide as well as considerate after-seals services. With our FSCP study tools' help, passing the exam will be a matter of course. It is our abiding belief to support your preparation of the FSCP study tools with enthusiastic attitude towards our jobs. And all efforts are paid off. Our FSCP Exam Torrent is highly regarded in the market of this field and come with high recommendation. Choosing our FSCP exam guide will be a very promising start for you to begin your exam preparation because our FSCP practice materials with high repute.

>> Reliable Exam FSCP Pass4sure <<

New Reliable Exam FSCP Pass4sure | High Pass-Rate Forescout Complete FSCP Exam Dumps: Forescout Certified Professional Exam

We all know that FSCP learning guide can help us solve learning problems. But if it is too complex, not only can't we get good results, but also the burden of students' learning process will increase largely. Unlike those complex and esoteric materials, our FSCP Preparation prep is not only of high quality, but also easy to learn. For our professional experts simplified the content of the FSCP exam questions for all our customers to be understood.

Forescout Certified Professional Exam Sample Questions (Q78-Q83):

NEW QUESTION # 78

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 in the Reports Portal
- B. Increase the "Purge Inactivity Timeout" setting
- C. Customize the message on the send syslog action

- D. Customize the message in the syslog configuration in Options > Core Ext > Syslog
- E. Configure a custom SNMP trap to be sent

Answer: C

Explanation:

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

NEW QUESTION # 79

Which field in the User Directory plugin should be configured for Active Directory subdomains?

- A. DNS Detection
- B. Address
- C. Parent Groups
- **D. Domain Aliases**
- E. Replicas

Answer: D

Explanation:

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

According to the Forescout User Directory Plugin Configuration Guide - Microsoft Active Directory Server Settings, the field that should be configured for Active Directory subdomains is "Domain Aliases".

Domain Aliases for Subdomains:

According to the Microsoft Active Directory Server Settings documentation:

"Configure the following additional server settings in the Directory and Additional Domain Aliases sections:

Domain Aliases - Configure additional domain names that users can use to log in, such as subdomains." Purpose of Domain Aliases:

According to the documentation:

Domain Aliases are used to specify:

- * Subdomains - Alternative domain names like subdomain.company.com
- * Alternative Domain Names - Other domain name variations
- * User Login Options - Additional domains users can use to authenticate
- * Alias Resolution - Maps aliases to the primary domain

Example Configuration:

For an organization with the primary domain company.com and subdomain accounts.company.com

* Domain Field - Set to: company.com

* Domain Aliases Field - Add: accounts.company.com

This allows users from either domain to authenticate successfully.

Why Other Options Are Incorrect:

- * A. Replicas - Replicas configure redundant User Directory servers, not subdomains
- * B. Address - Address field specifies the server IP/FQDN, not domain aliases
- * C. Parent Groups - Parent Groups relate to group hierarchy, not domain subdomains
- * E. DNS Detection - DNS Detection is not a User Directory configuration field

Additional Domain Configuration:

According to the documentation:

text

Primary Configuration:

```
## Domain: company.com
## Domain Aliases: accounts.company.com
# services.company.com
# mail.company.com
## Port: 636 (default)
```

Referenced Documentation:

- * Microsoft Active Directory Server Settings
- * Define User Directory Servers - Domain Aliases section

NEW QUESTION # 80

Main rules are executed independently of each other. However, one policy may be set to run first by configuring which of the following?

- A. Categorizing the Policy as an assessment policy
- B. Using Irresolvable criteria
- **C. Categorizing the Policy as a classifier**
- D. Setting the Main Rule condition to utilize primary classification
- E. There is no way to cause one policy to run first

Answer: C

Explanation:

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

According to the Forescout Administration Guide, one policy can be set to run first by categorizing the Policy as a classifier.

Classifier policies run before other policy types.

Policy Categorization and Execution Order:

According to the Forescout Administration Guide:

Forescout supports different policy categories, and these categories determine execution order:

* Classifier Policies - Run FIRST

* Used for initial device classification

* Establish basic device properties (OS, Function, Network Function)

- * Must complete before other policies can evaluate classification properties
- * Assessment Policies - Run AFTER classifiers
- * Assess compliance based on classified properties
- * Depend on classifier output
- * Control/Action Policies - Run LAST
- * Apply remediation actions
- * Depend on assessment results

How Classifier Policies Run First:

According to the documentation:

"When you categorize a policy as a classifier, it runs before assessment and action policies. This allows the classified properties to be established before other policies attempt to evaluate them" Reason for Classifier Priority:

According to the policy execution guidelines:

Classifier policies must run first because:

- * Dependency Resolution - Other policies depend on classification properties
- * Property Population - Classifiers populate device properties used by other policies
- * Execution Efficiency - Classifiers determine what type of device is being evaluated
- * Logical Flow - You must know what a device is before assessing or controlling it Why Other Options Are Incorrect:
 - * A. There is no way to cause one policy to run first - Incorrect; categorization determines execution order
 - * B. Setting Main Rule condition to utilize primary classification - While main rule conditions can reference classification, this doesn't change policy execution order
 - * C. Categorizing the Policy as an assessment policy - Assessment policies run AFTER classifier policies, not first
 - * E. Using Irresolvable criteria - Irresolvable criteria handling doesn't affect policy execution order Policy Categorization Example:

According to the documentation:

text

Policy Execution Order:

1. CLASSIFIER Policies (Run First)
 - "Device Classification Policy" (categorized as Classifier)
 - Resolves: OS, Function, Network Function
2. ASSESSMENT Policies (Run Second)
 - "Windows Compliance Policy" (categorized as Assessment)
 - Depends on classification from step 1
3. ACTION Policies (Run Last)
 - "Remediate Non-Compliant Devices" (categorized as Control)
 - Depends on assessment from step 2

In this workflow, because "Device Classification Policy" is categorized as a Classifier, it executes first, populating device properties that the subsequent Assessment and Action policies need.

Referenced Documentation:

- * ForeScout CounterACT Administration Guide - Policy Categorization
- * Categorize Endpoint Authorizations - Policy Categories and Execution

NEW QUESTION # 81

What should you do first when preparing for an upgrade to a new CounterACT version?

- A. Upgrading an appliance is done through Options/Modules.
- B. **Consult the CounterACT Release Notes for the appropriate version**
- C. From the appliance CLI, fstool upgrade /tmp/counteract-v8.0.1.fsp
- D. Upgrade only the modules compatible with the version you are installing.
- E. Upgrade the members first before upgrading the EM.

Answer: B

Explanation:

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

According to the Forescout Upgrade Guides for multiple versions, the first thing you should do when preparing for an upgrade to a new CounterACT version is consult the CounterACT Release Notes for the appropriate version.

Release Notes as First Step:

According to the official documentation:

"Review the Forescout Release Notes for important information before performing any upgrade." The documentation emphasizes this as a critical first step before any other upgrade activities.

What Release Notes Contain:

According to the upgrade guidance:

The Release Notes provide essential information including:

- * Upgrade Paths - Which versions you can upgrade from and to
- * Pre-Upgrade Requirements - System requirements and prerequisites
- * End-of-Life Products - Products that must be uninstalled before upgrade
- * Non-Supported Products - Products not compatible with the new version
- * Module/Plugin Dependencies - Version compatibility requirements
- * Known Issues - Potential problems and workarounds
- * Upgrade Procedures - Step-by-step instructions
- * Rollback Information - How to revert if needed

Critical Pre-Upgrade Information:

According to the Release Notes guidance:

"The upgrade process does not continue when end-of-life products are detected." Release Notes list:

- * End-of-Life (EOL) Products - Must be uninstalled before upgrade
- * Non-Supported Products - Must be uninstalled before upgrade
- * Plugin Version Compatibility - Which plugin versions work with the new Forescout version Upgrade Order vs. Release Notes Review:

According to the documentation:

While the order of upgrade (EM first, then Appliances) is important, consulting Release Notes comes FIRST because it determines what needs to be done before any upgrade attempts.

The Release Notes tell you:

- * Whether you can upgrade at all
- * What must be uninstalled
- * System requirements
- * Compatibility information

Only AFTER reviewing Release Notes do you proceed with the actual upgrade sequence.

Why Other Options Are Incorrect:

- * A. Upgrade the members first before upgrading the EM - This is the OPPOSITE of correct order; EM (Enterprise Manager) should be upgraded first
- * B. Upgrading an appliance is done through Options/Modules - This is not the upgrade path; upgrades are done through Tools > Options > CounterACT Devices
- * C. From the appliance CLI, fstool upgrade /tmp/counteract-v8.0.1.fsp - This is ONE possible upgrade method, but not the first step; downloading and reviewing Release Notes comes first
- * E. Upgrade only the modules compatible with the version you are installing - This is a consideration found IN the Release Notes, not the first step itself

Correct Upgrade Sequence:

According to the comprehensive upgrade documentation:

text

1. FIRST: Review Release Notes (determine what's needed)
2. Second: Check system requirements
3. Third: Uninstall EOL/non-supported products
4. Fourth: Back up Enterprise Manager and Appliances
5. Fifth: Upgrade Enterprise Manager
6. Sixth: Upgrade Appliances

Referenced Documentation:

- * Before You Upgrade the Forescout Platform - v8.3
- * Before You Upgrade the Forescout Platform - v9.1.2
- * Forescout 8.1.3 Release Notes
- * Installation Guide v8.0 - Upgrade section

NEW QUESTION # 82

Which of the following are included in System backups?

- A. Policies
- B. Hostname and IP address
- C. Wireless Plugin version 1.4.0 and above
- D. Failover Clustering plugin
- E. Switch Plugin version 8.7.0 and above

Answer: A

Explanation:

Comprehensive and Detailed Explanation From Exact Extract of Forescout Platform Administration and Deployment:
According to the Forescout Upgrade Guide and System Backup documentation, Policies are included in System backups.

What System Backups Include:

According to the official documentation:

"Each backup saves all Forescout Platform device and Console settings. This data includes the following:

- * Configuration
- * License
- * Operating System settings
- * Policies
- * Profiles
- * Reports
- * Administrator accounts
- * And other system data"

System Backup Contents:

According to the backup documentation:

System backups include:

- * Policies - All configured policies and policy templates
- * Configuration - System configuration settings
- * License Information - License keys and licensing data
- * Administrator Accounts - User accounts and access controls
- * Reports - Scheduled and saved reports
- * System Settings - Mail, network, and other system configurations
- * Profiles - User profiles and system profiles

What System Backups DO NOT Include:

According to the documentation:

System backups are encrypted using AES-256 and include most system data but are separate from

- * Appliance-specific firmware - May require separate backup
- * Component-specific backups - Some modules have separate backup procedures
- * Log files - Not typically included in system backups

Why Other Options Are Incorrect:

- * A. Switch Plugin version 8.7.0 and above - Plugin versions are not individually backed up; plugins are part of the module installation, not system configuration backup
- * C. Hostname and IP address - While these are part of system configuration, they are covered under "Configuration" not listed separately in backup contents
- * D. Failover Clustering plugin - Plugin software itself is not backed up; configuration related to plugins is backed up
- * E. Wireless Plugin version 1.4.0 and above - Plugin versions are installed separately; backups contain configuration, not plugin versions

Policy Backup Importance:

According to the documentation:

Policies are one of the most critical items included in system backups because:

- * Restore Capability - After system recovery, policies are restored automatically
- * Business Continuity - Restoring policies ensures the same security posture
- * Compliance - Policies contain compliance rules that must be preserved

* Operational Continuity - Restores endpoint management immediately after recovery System vs. Component Backups:

According to the backup documentation:

- * System Backup - Includes policies, configuration, licenses, administrator accounts, etc.
- * Component Backup - Specific modules may have additional backup capabilities
- * Both backup types - Both are encrypted with AES-256 for security

Backup Encryption:

According to the documentation:

"Both system and component backup files, backed up either manually or via a schedule, are encrypted using AES-256 to protect sensitive file data." This ensures that backed-up policies and other sensitive configuration remain secure.

Referenced Documentation:

- * Back Up your Enterprise Manager and/or Appliances - v8.4
- * Back Up your Enterprise Manager and/or Appliances - v8.5.1
- * Backing Up System and Component Settings - v8.4
- * Backing Up Forescout Platform System and Component Settings - v8.5.1

Lead2PassExam assists people in better understanding, studying, and passing more difficult certification exams. We take pride in successfully servicing industry experts by always delivering safe and dependable FSCP exam preparation materials. For your convenience, Lead2PassExam has prepared authentic Forescout Certified Professional Exam (FSCP) exam study material based on a real exam syllabus to help candidates go through their FSCP exams.

Complete FSCP Exam Dumps: <https://www.lead2passexam.com/Forescout/valid-FSCP-exam-dumps.html>

And to meet the challenges or pass a difficult FSCP exam we need to equip ourselves with more practical knowledge, advanced skills or some certificates of course. Now, do not seek with aimless, please pay attention to FSCP exam practice dumps. As we all know the passing rate is really low and the exam cost is expensive, if you fail once and you need to pay much attention and twice or more exam cost, purchasing our FSCP guide torrent materials can help you pass exams at first shot, Maybe Lead2PassExam will help you pass the FSCP dumps actual test easily and reduce your time and money.

Use modules in your code, Trash can friends, And to meet the challenges or pass a difficult FSCP Exam we need to equip ourselves with more practical knowledge, advanced skills or some certificates of course.

FSCP Exam Simulation: Forescout Certified Professional Exam & FSCP Certification Training

Now, do not seek with aimless, please pay attention to FSCP exam practice dumps, As we all know the passing rate is really low and the exam cost is expensive, if you fail once and you need to pay much attention and twice or more exam cost, purchasing our FSCP guide torrent materials can help you pass exams at first shot.

Maybe Lead2PassExam will help you pass the FSCP dumps actual test easily and reduce your time and money, All content are arranged legibly.