KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **FSCP**

Title : Forescout Certified Professional

Version : DEMO

1.Which CLI command gathers historical statistics from the appliance and outputs the information to a single *.csv file for processing and analysis?
A. fstool tech-support
B. fstool appstats
C. fstool va stats
D. fstool stats
E. fstool sysinfo stats
Answer: E
Explanation:
Comprehensive and Detailed Explanation From Exact Extract of Forescout Platform Administration and Deployment:
The fstool sysinfo stats command is the correct CLI command used in Forescout platforms to gather and export historical statistics from the appliance to a single CSV file for processing and analysis.
According to the Forescout CLI Commands Reference Guide (versions 8.1.x through 8.5.3), the fstool sysinfo command is listed under the Machine Administration category of fstool commands. The command's primary purpose is to "View Extensive System Information about the Appliance".
When used with the stats parameter, the command fstool sysinfo stats specifically:
Gathers historical statistics - The command collects comprehensive time-series data and historical statistics from the Forescout appliance
Outputs to a CSV file - The information is exported to a *single .csv file format, making it suitable for import into spreadsheet applications and data analysis tools
Enables processing and analysis - The CSV format allows administrators and engineers to perform offline analysis, trend analysis, and detailed troubleshooting
Why Other Options Are Incorrect:
fstool tech-support - This command is used to send logs and diagnostic information to Forescout Customer Support, not to output appliance statistics
fstool appstats - This command is not documented in any official Forescout CLI reference guides
fstool va stats - This command variant is not a recognized fstool command in Forescout documentation
fstool stats - This standalone command variant is not a recognized fstool command in Forescout documentation
Referenced Documentation:
Forescout CLI Commands Reference Guide v8.1.x, 8.2.x, 8.4.x, 8.5.2, and 8.5.3
Forescout Administration Guide v8.3 and v8.4
Machine Administration fstool Commands section - Forescout Official Documentation Portal

2.When using Remote Inspection for Windows, which of the following properties require fsprocsvc.exe interactive scripting?
A. User Directory Common Name
B. Update Microsoft Vulnerabilities
C. Windows Expected Script Result
D. Antivirus Running
E. Windows Service Running
Answer: C
Explanation:

Comprehensive and Detailed Explanation From Exact Extract of Forescout Platform Administration and Deployment:
The Windows Expected Script Result property is the correct answer. According to the official Forescout CounterACT Endpoint Module: HPS Inspection Engine Configuration Guide Version 10.8, the fsprocsvc.exe service is required to run interactive scripts for several CounterACT tasks during Remote Inspection operations on Windows endpoints.
The documentation explicitly lists the following Properties requiring the fsprocsvc service (with Remote Inspection, i.e., not via SecureConnector):
Windows Expected Script Result ✓
Device Interfaces
Number of IP Addresses
External Devices
Windows File MD5 Signature
Windows Is Behind NAT
Microsoft Vulnerabilities
About fsprocsvc.exe Service:
The fsprocsvc.exe service is a proprietary ForeScout service utility that is downloaded by the HPS Inspection Engine to endpoints. It is used to run interactive scripts for several CounterACT tasks. Key characteristics include:
Size on disk: Approximately 250KB
Memory acquired during runtime: 2 MB
Runs under: System context
Start type: Automatic
Inactivity timeout: After 2 hours of inactivity, the service stops automatically
Communication: Does not open any new network connection. Communication is carried out over Microsoft's SMB/RPC (445/TCP and 139/TCP) with domain credentials authentication
Why Other Options Are Incorrect:
A. User Directory Common Name - This property is derived from User Directory plugin queries and does not require fsprocsvc interactive scripting
B. Update Microsoft Vulnerabilities - This is an action, not a property. While Microsoft Vulnerabilities property does require fsprocsvc, "Update" is not the property name listed
D. Antivirus Running - This is a basic WMI-based property that does not require interactive scripting via fsprocsvc
E. Windows Service Running - This is a basic property that can be determined through WMI queries without requiring fsprocsvc interactive scripting
Interactive Scripts Requirement:
According to the HPS Inspection Engine Configuration Guide, WMI does not support interactive scripts on all Windows endpoints. When WMI is used for Remote Inspection, CounterACT uses the fsprocsvc service to run interactive scripts on endpoints that require them. The Windows Expected Script Result property specifically requires running a custom script on the endpoint, which necessitates the fsprocsvc service for proper execution.
Referenced Documentation:
Forescout CounterACT Endpoint Module: HPS Inspection Engine Configuration Guide Version 10.8
Section: "About fsprocsvc.exe" and "Properties requiring the service (With remote inspection, i.e. not via

SecureConnector)"

3.Which of the following is true regarding the Windows Installed Programs property which employs the "for any/for all" logic mechanism?
A. Although the condition has multiple sub-properties, when "ANY" is selected it evaluates the programs for any of the configured sub-properties.
B. The condition does not have any sub-properties. The "any/all" refers to the multiple programs.
C. Although the condition has sub-properties which could refer to a single program on multiple endpoints, the "any/all" refers to the program's properties.
D. Although the condition has multiple sub-properties, the "any/all" refers to the sub-properties and not the programs.
E. Although the condition has multiple sub-properties, the "any/all" refers to the programs and not the sub-properties.
Answer: E
Explanation:
Comprehensive and Detailed Explanation From Exact Extract of Forescout Platform Administration and Deployment:
The Windows Installed Programs property condition utilizes multiple sub-properties including Program Name, Program Version, Program Vendor, and Program Path. However, when using the "for ANY/for ALL" logic mechanism, the "any/all" refers to the PROGRAMS and not to the sub-properties.
How the "Any/All" Logic Works with Windows Installed Programs:
When configuring a policy condition with the Windows Installed Programs property, the "any/all" logic determines whether an endpoint should match the condition based on:
"For ANY" - The endpoint matches the policy condition if ANY of the configured programs are installed on the endpoint
"For ALL" - The endpoint matches the policy condition if ALL of the configured programs are installed on the endpoint
Example: If an administrator creates a condition like:
Windows Installed Programs contains "Microsoft Office" OR "Adobe Reader"
Using "For ANY": The endpoint matches if it has EITHER Microsoft Office OR Adobe Reader installed
Using "For ALL": The endpoint matches only if it has BOTH Microsoft Office AND Adobe Reader installed
The sub-properties (Program Name, Version, Vendor, Path) are used to define and identify which specific programs to match against, but the "any/all" logic applies to the PROGRAMS themselves, not to the sub-properties.
Why Other Options Are Incorrect:
A - Incorrectly states the "any/all" evaluates the programs for the sub-properties
B - Factually incorrect; the condition definitely has multiple sub-properties (Name, Version, Vendor, Path)
C - Confuses the scope; the "any/all" does not refer to "program's properties" but to multiple programs
D - Inverted logic; the "any/all" refers to the programs, not the sub-properties
Referenced Documentation:
Forescout Administration Guide v8.3, v8.4
Working with Policy Conditions - List of Properties by Category
Windows Applications Content Module Configuration Guide

4.What is the best practice to pass an endpoint from one policy to another?
A. Use operating system property
B. Use sub rules
C. Use function property
D. Use groups
E. Use policy condition
Answer: B
Explanation:
Comprehensive and Detailed Explanation From Exact Extract of Forescout Platform Administration and Deployment:
According to the Forescout Platform Administration and Deployment Documentation, the best practice to pass an endpoint from one policy to another is to use SUB-RULES.
Sub-Rules and Policy Routing:
Sub-rules are conditional branches within a Forescout policy that allow for sophisticated endpoint routing and handling. When an endpoint matches a sub-rule condition, it can be directed to perform specific actions or be passed to another policy group for further evaluation.
Key Advantages of Using Sub-Rules:
Granular Control - Sub-rules enable precise segmentation of endpoints based on multiple properties and conditions
Hierarchical Processing - Once an endpoint matches a sub-rule, it proceeds down the sub-rule branch; later sub-rules of the policy are not evaluated for that endpoint
Efficient Endpoint Routing - Sub-rules allow endpoints to be efficiently routed to appropriate policy handlers without evaluating unnecessary conditions
Policy Chaining - Sub-rules facilitate the logical flow and routing of endpoints through multiple policy layers
Best Practice Implementation:
The documentation emphasizes that when designing policies for endpoint management, administrators should:
Use sub-rules to create conditional branches that evaluate endpoints against multiple criteria Route endpoints to appropriate policy handlers based on their properties and compliance status Avoid using simple property-based routing when complex multi-step evaluation is needed Why Other Options Are Incorrect:
A. Use operating system property - While OS properties can be used in conditions, they are not the mechanism for passing endpoints between policies
C. Use function property - Function properties are not used for inter-policy endpoint routing
D. Use groups - While groups are useful for organizing endpoints, they are not the primary best practice for passing endpoints between policies
E. Use policy condition - Policy conditions define what endpoints should be evaluated, but sub-rules provide the actual routing mechanism
Referenced Documentation:
Forescout Platform Administration Guide - Defining Policy Sub-Rules "Defining Forescout Platform Policy Sub-Rules" - Best Practice section Sub-Rule Advanced Options documentation

5.Which of the following User Directory server settings is necessary to enable guest approval by

sponsors?
A. Policy to control
B. Guest Tags
C. Sponsor Group
D. Guest password policy
E. Authentication Server
Answer: C
Explanation:
Comprehensive and Detailed Explanation From Exact Extract of Forescout Platform Administration and Deployment:
The Sponsor Group is the necessary User Directory server setting required to enable guest approval by sponsors. According to the Forescout User Directory Plugin Configuration Guide and Guest Management Portal documentation, Sponsor Groups must be created and configured to define the corporate employees (sponsors) who are authorized to approve or decline guest network access requests.
Sponsor Group Configuration:
In the Guest Management pane, the Sponsors tab is used to define the corporate employees who are authorized to log into the Guest Management Portal to approve network access requests from guests. These employees are assigned to specific Sponsor Groups, which control which sponsors can approve guest access requests.
How Sponsor Groups Enable Guest Approval:
Sponsor Definition - Corporate employees must be designated as sponsors and assigned to a Sponsor Group
Approval Authority - Sponsors in assigned groups can approve or decline guest network access requests
Authentication - When "Enable sponsor approval without authentication via emailed link" is selected, sponsors in the designated group can approve guests based on email link authorization
Guest Registration - Guest registration options connect Sponsor Groups to the guest approval workflow
Why Other Options Are Incorrect:
A. Policy to control - While policies are used for guest control, they do not define which sponsors can approve guests
B. Guest Tags - Guest Tags are used to classify and organize guest accounts, not to enable sponsor approval
D. Guest password policy - This setting controls password requirements for guests, not sponsor approval authority
E. Authentication Server - Authentication servers verify credentials but do not establish sponsor approval groups
Referenced Documentation:
Forescout User Directory Plugin Configuration Guide - Create Sponsors section Guest Management Portal - Sponsor Configuration documentation "Create sponsors" - Forescout Administration Guide section