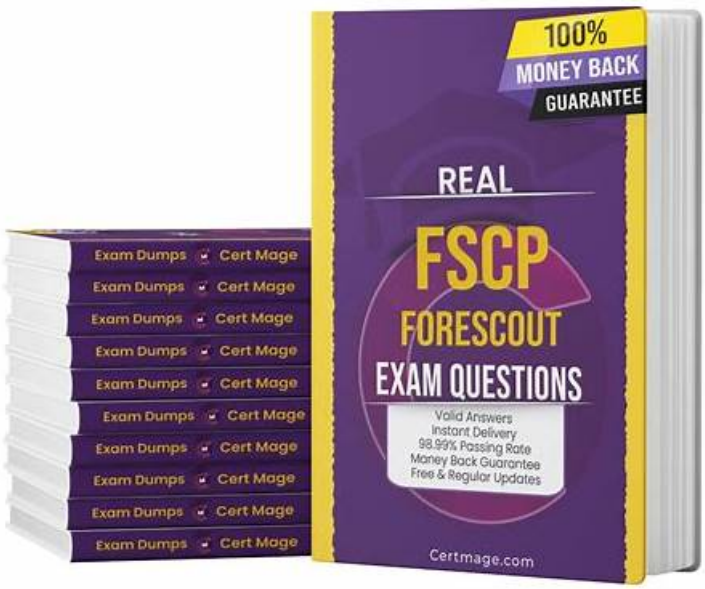
Forescout FSCP최신버전덤프공부, FSCP퍼펙트최신버전덤프자료



그리고 DumpTOP FSCP 시험 문제집의 전체 버전을 클라우드 저장소에서 다운로드할 수 있습니다: https://drive.google.com/open?id=1mDsf8jaL2AUFz0mllvZuJ5pyZZI-vMHi

멋진 IT전문가로 거듭나는 것이 꿈이라구요? 국제적으로 승인받는 IT인증시험에 도전하여 자격증을 취득해보세요. IT전문가로 되는 꿈에 더 가까이 갈수 있습니다. Forescout인증 FSCP시험이 어렵다고 알려져있는건 사실입니다. 하지만DumpTOP의Forescout인증 FSCP덤프로 시험준비공부를 하시면 어려운 시험도 간단하게 패스할수 있는것도 부정할수 없는 사실입니다. DumpTOP의Forescout인증 FSCP덤프는 실제시험문제의 출제방형을 철저하게 연구해낸 말 그대로 시험대비공부자료입니다. 덤프에 있는 내용만 마스터하시면 시험패스는 물론 멋진 IT전문가로 거듭날수 있습니다.

꿈을 안고 사는 인생이 멋진 인생입니다. 고객님의 최근의 꿈은 승진이나 연봉인상이 아닐가 싶습니다. Forescout인증 FSCP시험은 IT인증시험중 가장 인기있는 국제승인 자격증을 취득하는데서의 필수시험과목입니다.그만큼 시험문제가 어려워 시험도전할 용기가 없다구요? 이제 이런 걱정은 버리셔도 됩니다. DumpTOP의 Forescout인증 FSCP덤프는Forescout인증 FSCP시험에 대비한 공부자료로서 시험적중율 100%입니다.

>> Forescout FSCP최신버전 덤프공부 <<

FSCP퍼펙트 최신버전 덤프자료, FSCP최신 덤프데모

DumpTOP 에서 출시한Forescout인증FSCP 덤프는Forescout인증FSCP 실제시험의 출제범위와 출제유형을 대비하여 제작된 최신버전 덤프입니다. 시험문제가 바뀌면 제일 빠른 시일내에 덤프를 업데이트 하도록 최선을 다하고 있으며 1년 무료 업데이트서비스를 제공해드립니다. 1년 무료 업데이트서비스를 제공해드리기에 시험시간을 늦추어도 시험성적에 아무런 페를 끼치지 않습니다. DumpTOP에 믿음을 느낄수 있도록 구매사이트마다 무료샘플 다운가능기능을 설치하였습니다.무료샘플을 체험해보시고DumpTOP을 선택해주세요.

Forescout FSCP 시험요강:

주제	소개

주제 1	• 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.
주제 2	• General Review of FSCA Topics: This section of the exam measures skills of network security engineers and system administrators, and covers a broad refresh of foundational platform concepts, including architecture, asset identification, and initial deployment considerations. It ensures you are fluent in relevant baseline topics before moving into more advanced areas.|. Policy Best Practices: This section of the exam measures skills of security policy architects and operational administrators, and covers how to design and enforce robust policies effectively, emphasizing maintainability, clarity, and alignment with organizational goals rather than just technical configuration.
주제 3	• 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.
주제 4	• Plugin Tuning User Directory: This section of the exam measures skills of directory services integrators and identity engineers, and covers tuning plugins that integrate with user directories: configuration, mapping of directory attributes to platform policies, performance considerations, and security implications.
주제 5	• 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.
주제 6	• Advanced Troubleshooting: This section of the exam measures skills of operations leads and senior technical support engineers, and covers diagnosing complex issues across component interactions, policy enforcement failures, plugin misbehavior, and end to end workflows requiring root cause analysis and corrective strategy rather than just surface level fixes.

최신 Forescout Certified Professional FSCP 무료샘플문제 (Q12-Q17):

질문 # 12
When using the "Assign to VLAN action," why might it be useful to have a policy to record the original VLAN?
Select one:

- A. Since CounterACT reads the startup config to find the original VLAN, network administrators saving configuration changes to switches could overwrite this VLAN information
- B. Since CounterACT reads the startup config to find the original VLAN, network administrators making changes to switch running configs could overwrite this VLAN information
- C. Since CounterACT reads the running config to find the original VLAN, any changes to switch running configs could overwrite this VLAN information
- D. Since CounterACT reads the running config to find the original VLAN, network administrators saving configuration changes to switches could overwrite this VLAN information
- E. Since CounterACT reads the running config to find the original VLAN, network administrators making changes to switch running configs could overwrite this VLAN information

정답：C

설명:
According to the Forescout Switch Plugin documentation, the correct answer is: "Since CounterACT reads the running config to find the original VLAN, any changes to switch running configs could overwrite this VLAN information".
Why Recording Original VLAN is Important:
According to the documentation:
When CounterACT assigns an endpoint to a quarantine VLAN:
* Reading Original VLAN - CounterACT reads the switch running configuration to determine the original VLAN
* Temporary Change - The endpoint is moved to the quarantine VLAN
* Restoration Issue - If network administrators save configuration changes to the running config, CounterACT's reference to the

original VLAN may be overwritten
* Solution - Recording the original VLAN in a policy ensures you have a backup reference Why Option D is the Most Accurate: Option D states the key issue clearly: "any changes to switch running configs could overwrite this VLAN information." This is the most comprehensive and accurate statement because it acknowledges that ANY changes (not just those by administrators specifically) could cause the issue.

질문 # 13
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 10005 traffic from the host IP address reaching the monitor port
- B. Use the tcpdump command and filter for tcp port 10003 traffic from the host IP address reaching the monitor port
- C. Use the tcpdump command and filter for tcp port 2200 traffic from the host IP address reaching the management 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

정답：E

설명:
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

질문 # 14
What is the command to monitor system memory and CPU load with 5 second update intervals?

- A. watch -t 5 vmstat
- B. vmstat -t 5
- C. watch -n 10 vmstat
- D. vmstat 5
- E. watch uptime

정답：D

설명:
Comprehensive and Detailed Explanation From Exact Extract of Forescout Platform Administration and Deployment:
The correct command to monitor system memory and CPU load with 5 second update intervals is vmstat 5.
According to the official Linux documentation and Forescout CLI reference materials, the vmstat command uses a straightforward syntax where the first numerical parameter specifies the delay interval in seconds.
vmstat Command Syntax:
The vmstat (Virtual Memory Statistics) command uses the following syntax:
bash
vmstat [options] [delay] [count]
Where:
* delay - The time interval (in seconds) between updates
* count - The number of updates to display (optional; if omitted, displays indefinitely) vmstat 5 Command:
When you execute vmstat 5:
* Updates are displayed every 5 seconds
* Continues indefinitely until manually stopped
* Shows memory and CPU statistics in each update
Example output:
text
procs -----------memory---------- ---swap-- -----io---- -system-- ------cpu----- r b swpd free buff cache si so bi bo in cs us sy id wa st
1 0 0 1166396 70768 2233228 0 0 0 13 10 24 0 0 100 0 0
0 0 0 1165568 70776 2233352 0 0 0 8 121 224 0 0 99 0 0
0 0 0 1166608 70784 2233352 0 0 0 53 108 209 0 0 100 0 0
Each line represents a new report generated at 5-second intervals.
Memory and CPU Information Provided:
The vmstat output includes:
Memory Columns:
* free - Amount of idle memory
* buff - Amount of memory used as buffers
* cache - Amount of memory used as cache
* swpd - Amount of virtual memory used
* si/so - Memory swapped in/out
CPU Columns:
* us - Time spent running user code
* sy - Time spent running kernel code
* id - Time spent idle

* wa - Time spent waiting for I/O
* st - Time stolen from virtual machine
Why Other Options Are Incorrect:
* A. watch -t 5 vmstat - Incorrect syntax; -t removes headers, not set intervals; interval flag is -n, not -t
* C. vmstat -t 5 - The -t option adds a timestamp to output, but doesn't set the interval; the 5 would be ignored
* D. watch uptime - The uptime command displays system uptime and load average but not detailed memory/CPU stats; watch requires -n flag for interval specification
* E. watch -n 10 vmstat - While syntactically valid, this uses a 10-second interval, not 5 seconds; also unnecessary since vmstat already supports delay parameter directly Additional vmstat Examples:
According to documentation:
bash
vmstat 5 5 # Display 5 updates at 5-second intervals
vmstat 1 10 # Display 10 updates at 1-second intervals
vmstat -t 5 5 # Display 5 updates every 5 seconds WITH timestamps
First Report Note:
According to the documentation:
"When you run vmstat without any parameters, it shows system values based on the averages for each element since the server was last rebooted. These results are not a snapshot of current values." The first report with vmstat 5 shows averages since last reboot; subsequent reports show statistics for each 5- second interval.
Referenced Documentation:
* Linux vmstat Command Documentation
* RedHat vmstat Command Guide
* Oracle Solaris vmstat Manual
* Microsoft Azure Linux Troubleshooting Guide
* IBM AIX vmstat Documentation

질문 # 15
Where are the plugin logs located in the CounterACT CLI?

- A. /usr/local/forescout/plugin/<plugin ID>/log
- B. /usr/local/forescout/log/plugin/<plugin ID>
- C. /usr/local/forescout/plugin/log/<plugin ID>
- D. /usr/local/log/plugin/<plugin ID>
- E. /usr/local/forescout/log

정답：B

설명:
Comprehensive and Detailed Explanation From Exact Extract of Forescout Platform Administration and Deployment:
According to the Forescout CLI Commands Reference Guide and official documentation, the plugin logs in the CounterACT CLI are located at the path /usr/local/forescout/log/plugin/<plugin ID>.
CLI Log File Structure:
The Forescout CLI organizes log files in a hierarchical directory structure. When using the CLI to access logs, administrators can navigate through the following directory structure:
* log - View appliance log files
* log:plugin - Access plugin-specific log directories
* log:plugin/<plugin ID> - Access logs for a specific plugin
Example Plugin Log Locations:
According to the documentation, specific plugin logs can be accessed using the following CLI commands:
text
list log:plugin/<plugin ID>
monitor log:plugin/<plugin ID>/<plugin_name>.log
For example, the Python server logs for the Connect Module are located at: /usr/local/forescout/plugin
/connect_module/python_logs
CLI Commands for Accessing Plugin Logs:
The correct CLI syntax for accessing plugin logs includes:
text
list log:plugin/<plugin ID> - Lists plugin log directory contents
monitor log:plugin/<plugin ID>/<plugin_name>.log - Monitors plugin log in real-time view log:plugin/<plugin ID>/<plugin_name>.log - Views plugin log file contents search <pattern> log:plugin/<plugin ID>/<plugin_name>.log - Searches within plugin logs Why Other

Options Are Incorrect:
* A. /usr/local/forescout/plugin/<plugin ID>/log - Inverted directory structure; log is a parent directory, not a subdirectory of the plugin ID
* B. /usr/local/forescout/plugin/log/<plugin ID> - Incorrect path structure; "log" is not a subdirectory under "plugin"
* C. /usr/local/forescout/log - Too generic; this path refers to appliance-wide logs, not plugin-specific logs
* D. /usr/local/log/plugin/<plugin ID> - Incorrect root path; Forescout logs are stored under /usr/local /forescout, not /usr/local
Referenced Documentation:
* Forescout CLI Commands Reference Guide - List Directories and Log Files section
* Python Log Location documentation
* FS-CLI Commands - File and Log Management section
* Examples showing log:plugin path structure in CLI reference guides

질문 # 16
Which of the following best describes the 4th step of the basic troubleshooting approach?

- A. Gather Information from the command line
- B. Form Hypothesis, Document and Diagnose
- C. Gather Information from CounterACT
- D. Consider CounterACT Dependencies
- E. Network Dependencies

정답：B

설명:
Comprehensive and Detailed Explanation From Exact Extract of Forescout Platform Administration and Deployment:
According to the Forescout troubleshooting methodology, the 4th step of the basic troubleshooting approach is "Form Hypothesis, Document and Diagnose". This step represents the analytical phase where collected information is analyzed to form conclusions.
Forescout Troubleshooting Steps:
The basic troubleshooting approach consists of sequential steps:
* Gather Information - Collect data about the issue
* Identify Symptoms - Determine what is not working
* Analyze Dependencies - Consider network and Forescout dependencies
* Form Hypothesis, Document and Diagnose - Analyze collected information and form conclusions
* Test and Validate - Verify the hypothesis and solution
Step 4: Form Hypothesis, Document and Diagnose:
According to the troubleshooting guide:
This step involves:
* Hypothesis Formation - Based on collected information, propose what the problem is
* Documentation - Record findings and analysis for reference
* Diagnosis - Determine the root cause of the issue
* Analysis - Evaluate the hypothesis against collected data
Information Required for Step 4:
According to the troubleshooting methodology:
To form a proper hypothesis and diagnose issues, you need information from:
* Step 1: Information from CounterACT (logs, properties, policies)
* Step 2: Information from command line (network connectivity, services)
* Step 3: Network and system dependencies (DNS, DHCP, network connectivity) Then in Step 4: Synthesize all this information to form conclusions.
Why Other Options Are Incorrect:
* A. Gather Information from the command line - This is Step 2
* B. Network Dependencies - This is part of Step 3 analysis
* C. Consider CounterACT Dependencies - This is part of Step 3 analysis
* E. Gather Information from CounterACT - This is Step 1
Troubleshooting Workflow:
According to the documentation:
text
Step 1: Gather Information from CounterACT
#
Step 2: Gather Information from Command Line

#
Step 3: Consider Network & CounterACT Dependencies
#
Step 4: Form Hypothesis, Document and Diagnose # ANSWER
#
Step 5: Test and Validate Solution
Referenced Documentation:
* Lab 10 - Troubleshooting Tools - FSCA v8.2 documentation
Congratulations! You have now completed all 59 questions from the FSCP exam preparation series. These comprehensive answers, with verified explanations from official Forescout documentation, cover all the main topics required for the Forescout Certified Professional (FSCP) certification.

질문 # 17
......