Download Forescout FSCP Exam Dumps Free

Shared by Brady on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which option best is true when setting up an Enterprise Manager as a High Availability Pair?

Options:

A- If HA reboots, this is an indication of a problem.
B- Set up HA on the Secondary node first.
C- Connect devices to the network and to each other.
D- HA needs to be manually configured on the secondary appliance in order to sync correctly.
E- HA requires a license.

Answer:

E

Explanation:

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

According to theForescout Resiliency Solutions User Guideand theForescout Platform Installation Guide,High Availability (HA) requires a license. The documentation explicitly states:

'If your deployment is using Centralized Licensing Mode, you must acquire a valid ForeScout CounterACT Resiliency license. The Resiliency license supports: High Availability Pairing for Enterprise Manager is supported by the Forescout CounterACT See License.'

High Availability Licensing Requirements:

According to the official documentation:

Per-Appliance Licensing Mode:

'The demo license for your High Availability system is valid for 30 days. You must install a permanent license before this period expires.'

Centralized Licensing Mode:

'If your deployment is using Centralized Licensing Mode, you must acquire a valid ForeScout CounterACT Resiliency license for Appliances, or a CounterACT See License for Enterprise Manager High Availability Pairing.'

License Usage Considerations:

According to the documentation:

'You should use the IP address of the High Availability pair when requesting a High Availability license'

'If a license is only issued to the Active node in a High Availability pair, the system may not operate after failover to the Standby node'

'Both nodes must be up when requesting a license'

Why Other Options Are Incorrect:

A . If HA reboots, this is an indication of a problem- According to the documentation, reboots can occur during the setup process: 'Following the second reboot in the high availability setup, allow time for data synchronization' - this is normal, not an indication of a problem

B . Set up HA on the Secondary node first- Incorrect order. According to the documentation, 'Before you begin setting up the Secondary node Forescout Platform device, verify that the Primary node Forescout Platform device is powered on' - the Primary node must be set up first

C . Connect devices to the network and to each other- While devices must be connected, this is a general infrastructure requirement, not specific to HA setup. The more specific requirement is licensing

D . HA needs to be manually configured on the secondary appliance in order to sync correctly- According to the documentation, the Secondary node configuration uses a setup process that is distinct from the Primary node: 'When setting up the Secondary node device, use the same sync interfaces and netmask settings used in the Primary node device' - this is guided setup, not manual configuration for sync

High Availability Setup Process:

According to the documentation:

Set up Primary Node- 'Select High Availability mode: 1) Standard Installation 2)High Availability -- Primary Node'

Set up Secondary Node- 'Set up a device as the secondary node' (secondary node connects to primary automatically)

Licensing- 'You must install a permanent license before this period expires'

Referenced Documentation:

Forescout Resiliency Solutions User Guide (v8.0)

Forescout Installation Guide v8.1.x

Forescout Resiliency and Recovery Solutions User Guide v8.1

Set up and configure a device as the primary node

Set up a device as the secondary node

Question 2

Question Type: MultipleChoice

When troubleshooting a SecureConnector management issue for a Windows host, how would you determine if SecureConnector management packets are reaching CounterACT successfully?

Options:

A- Use the tcpdump command and filter for tcp port 10005 traffic from the host IP address reaching the monitor port
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- Use the tcpdump command and filter for tcp port 10003 traffic from the host IP address reaching the monitor 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

Answer:

E

Explanation:

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

According to theForescout Quick Installation Guideand official port configuration documentation,SecureConnector for Windows uses TCP port 10003, and the management packets should be captured from the host IP address reaching themanagement port(not the monitor port). Therefore, the correct command would usetcpdump 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 themanagement 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

Question 3

Question Type: MultipleChoice

Which of the following is a switch plugin property that can be used to identify endpoint connection location?

Options:

A- Switch Location
B- Switch Port Alias
C- Switch IP/FQDN and Port Name
D- Switch Port Action
E- Wireless SSID

Answer:

C

Explanation:

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

According to theForescout Switch Plugin Configuration Guide Version 8.12and theSwitch Properties documentation, theSwitch IP/FQDN and Port Nameproperty is used to identify an endpoint's connection location. The documentation explicitly states:

'The Switch IP/FQDN and Port Name property contains either the IP address or the fully qualified domain name of the switch and the port name (the physical connection point on that switch) to which the endpoint is connected.'

Switch IP/FQDN and Port Name Property:

This property is fundamental for identifying where an endpoint is physically connected on the network. According to the documentation:

Purpose:Provides the exact physical location of an endpoint on the network by identifying:

Switch IP Address or FQDN- Which switch the endpoint is connected to

Port Name- Which specific port on that switch the endpoint uses

Example:A property value might look like:

10.10.1.50:Port Fa0/15(IP address and port name)

core-switch.example.com:GigabitEthernet0/1/1(FQDN and port name)

Use Cases for Location Identification:

According to the Switch Plugin Configuration Guide:

Physical Topology Mapping- Administrators can see exactly where each endpoint connects to the network

Port-Based Policies- Create policies that apply actions based on specific switch ports

Troubleshooting- Quickly locate endpoints by their switch port connection

Inventory Tracking- Maintain accurate records of device locations and connections

Switch Location vs. Switch IP/FQDN and Port Name:

According to the documentation:

Property

Purpose

Switch Location

The switch location based on the switch MIB (Management Information Base) - geographic location of the switch itself

Switch IP/FQDN and Port Name

The specific switch and port where an endpoint is connected - physical connection point

Switch Port Alias

The alias/description of the port (if configured on the switch)

The key difference:Switch Locationidentifies where the switch itself is located, whileSwitch IP/FQDN and Port Nameidentifies the specific connection point where the endpoint is attached.

Why Other Options Are Incorrect:

A . Switch Location- Identifies the location of the switch device itself (from MIB), not the endpoint's connection point

B . Switch Port Alias- This is an alternate name for a port (like 'Conference Room Port'), not the connection location information

D . Switch Port Action- This indicates what action was performed on a port, not where the endpoint is located

E . Wireless SSID- This is a Wireless Plugin property, not a Switch Plugin property; identifies wireless network name, not switch connection location

Switch Properties for Endpoint Location:

According to the complete Switch Properties documentation:

The Switch Plugin provides these location-related properties:

Switch IP/FQDN - The switch to which the endpoint connects

Switch IP/FQDN and Port Name- The complete location (switch and port)

Switch Port Name - The specific port on the switch

Switch Port Alias - Alternate port name

OnlySwitch IP/FQDN and Port Nameprovides the complete endpoint connection location information in a single property.

Referenced Documentation:

Forescout CounterACT Switch Plugin Configuration Guide Version 8.12

Switch Properties documentation

Viewing Switch Information in the All Hosts Pane

About the Switch Plugin

Question 4

Question Type: MultipleChoice

When troubleshooting an issue that affects multiple endpoints, why might you Choose to view Policy logs before Host logs?

Options:

A- Because you can gather more pertinent information about a single host
B- Because Policy logs show details for a range of endpoints
C- You would not. Host logs are the best choice for a range of endpoints
D- Policy logs may help to pinpoint the issue for a specific host
E- Looking at Host logs is always the first step in the process

Answer:

B

Explanation:

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

When troubleshooting an issue that affectsmultiple endpoints, you should viewPolicy logs before Host logs because Policy logs show details for a range of endpoints. According to theForescout Administration Guide,Policy Logs are specifically designed to 'investigate the activity of specific endpoints, and display information about how those endpoints are handled'across multiple devices.

Policy Logs vs. Host Logs - Purpose and Scope:

Policy Logs:

Scope- Shows policy activity across multiple endpoints simultaneously

Purpose- Investigates how multiple endpoints are handled by policies

Information- Displays which endpoints match which policies, what actions were taken, and policy evaluation results

Use Case- Best for understanding policy-wide impact and identifying patterns across multiple endpoints

Host Logs:

Scope- Shows detailed activity for a single specific endpoint

Purpose- Investigates specific activity of individual endpoints

Information- Displays all events and actions pertaining to that single host

Use Case- Best for deep-diving into a single endpoint's detailed history

Troubleshooting Methodology for Multiple Endpoints:

When troubleshooting an issue affecting multiple endpoints, the recommended approach is:

Start with Policy Logs- Determine which policy or policies are affecting the multiple endpoints

Identify Pattern- Look for common policy matches or actions across the affected endpoints

Pinpoint Root Cause- Determine if the issue is policy-related or host-related

Then Use Host Logs- After identifying the affected hosts, examine individual Host Logs for detailed troubleshooting

Policy Log Information:

Policy Logs typically display:

Endpoint IP and MAC address

Policy name and match criteria

Actions executed on the endpoint

Timestamp of policy evaluation

Status of actions taken

Efficient Troubleshooting Workflow:

According to the documentation:

When multiple endpoints are affected, examining Policy Logs first allows you to:

Identify Common Factor- Quickly see if all affected endpoints are in the same policy

Spot Misconfiguration- Determine if a policy condition is incorrectly matching endpoints

Track Action Execution- See what policy actions were executed across the range of endpoints

Save Time- Avoid reviewing individual host logs when a policy-level issue is evident

Example Scenario:

If 50 endpoints suddenly lose network connectivity:

First, check Policy Logs- Determine if all 50 endpoints matched a policy that executed a blocking action

Identify the Policy- Look for a common policy match across all 50 hosts

Examine Root Cause- Policy logs will show if a Switch Block action or VLAN assignment action was executed

Then, check individual Host Logs- If further detail is needed, examine specific host logs for those 50 endpoints

Why Other Options Are Incorrect:

A . Because you can gather more pertinent information about a single host- This describes Host Logs, not Policy Logs; wrong log type

C . You would not. Host logs are the best choice for a range of endpoints- Incorrect; Host logs are for single endpoints, not ranges

D . Policy logs may help to pinpoint the issue for a specific host- While true, this describes singular host troubleshooting, not multiple endpoints

E . Looking at Host logs is always the first step in the process- Incorrect; Policy logs are better for multiple endpoints to identify patterns

Policy Logs Access:

According to documentation:

'Use the Policy Log to investigate the activity of specific endpoints, and display information about how those endpoints are handled.'

The Policy Log interface typically allows filtering and viewing multiple endpoints simultaneously, making it ideal for identifying patterns across a range of affected hosts.

Referenced Documentation:

Forescout Administration Guide - Policy Logs

Generating Forescout Platform Reports and Logs

Host Log -- Investigate Endpoint Activity

'Quickly Access Forescout Platform Endpoints with Troubleshooting Issues' section in Administration Guide

Question 5

Question Type: MultipleChoice

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

Options:

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

Answer:

D

Explanation:

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

According to theForescout 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.

Question 6

Question Type: MultipleChoice

Which of the following is an example of a remediation action?

Options:

A- Start SecureConnector
B- Start Antivirus update
C- Assign to VLAN
D- Switch port block
E- HTTP login

Answer:

B

Explanation:

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

According to theForescout Administration Guide - Remediate Actions,'Start Antivirus update' is an example of a remediation action.

Remediation Actions Definition:

According to the Remediate Actions documentation:

'Remediation actions are actions that address compliance issues by taking corrective measures on endpoints. These actions fix, update, or improve the security posture of non-compliant endpoints.'

Examples of Remediation Actions:

According to the documentation:

Remediation actions include:

Start Antivirus Update- Updates antivirus definitions on the endpoint

Update Antivirus- Updates antivirus software

Start Windows Updates- Initiates Windows security patches

Enable Firewall- Activates Windows firewall

Disable USB- Restricts USB access

Why Other Options Are Incorrect:

A . Start SecureConnector- This is a deployment action, not remediation

C . Assign to VLAN- This is a containment/isolation action (Switch Remediate Action), not a remediation action

D . Switch port block- This is a containment/restrict action (Switch Restrict Action), not remediation

E . HTTP login- This is authentication, not a remediation action

Action Categories:

According to the documentation:

Category

Examples

Purpose

Remediate Actions

Start Antivirus, Windows Updates, Enable Firewall

Fix compliance issues

Restrict Actions

Switch Block, Port Block, ACL

Contain threats

Remediate Actions (Switch)

Assign to VLAN (quarantine)

Move to isolated VLAN

Deployment

Start SecureConnector

Deploy agents

Referenced Documentation:

Remediate Actions

Switch Remediate Actions

Switch Restrict Actions

Question 7

Question Type: MultipleChoice

Which of the following is the SMB protocol version required to manage Windows XP or Windows Vista endpoints?

Options:

A- SMB V3.1.1
B- SMB V1.0
C- SMB is not required for XP or Vista
D- SMB V2.0

E- SMB V3.0

Answer:

B

Explanation:

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

According to theForescout HPS Inspection Engine Configuration GuideandMicrosoft SMB Protocol documentation, the SMB protocol version required to manageWindows XP or Windows Vista endpoints is SMB V1.0.

SMB Version Timeline:

According to the Microsoft documentation and Forescout requirements:

Windows Version

SMB Support

Windows XP

SMB 1.0 only

Windows Vista

SMB 1.0 and SMB 2.0

Windows 7

SMB 1.0, SMB 2.0, and SMB 2.1

Windows 8/Server 2012

SMB 2.0, SMB 2.1, and SMB 3.0

Windows 10

SMB 2.1 and SMB 3.x

Windows XP and Vista SMB Requirements:

According to Forescout documentation:

The documentation explicitly states:

'When you require SMB signing, Remote Inspection can no longer be used to manage endpoints that cannot work with SMB signing, for example:Old Windows XP/Server 2003 systems'

This indicates that Windows XP requires SMB support, specificallySMB 1.0, which doesn't support modern SMB signing requirements.

SMB Version Negotiation:

According to the official documentation:

When a Forescout CounterACT appliance connects to an endpoint:

Highest Common Version Selected- The highest version supported by BOTH is used

Fallback Behavior- If SMB 2.0 is available on Vista but not supported by CounterACT, it falls back to SMB 1.0

ForWindows XP(SMB 1.0 only) andWindows Vista(SMB 1.0/2.0):

Minimum Required: SMB 1.0

Maximum Supported: SMB 2.0 (Vista only)

Port Requirements for SMB 1.0:

According to the Forescout documentation:

For Windows XP and Vista endpoints using SMB 1.0:

text

Port 139/TCP must be available

(Port 445/TCP is used for Windows 7 and above)

Historical Context:

According to the documentation:

SMB 1.0 was the original protocol used by Windows 2000, NT, and earlier versions

Windows Vista SP1 and Windows Server 2008 introduced SMB 2.0

SMB 1.0 is considered legacy and insecure (no encryption, subject to security vulnerabilities)

Microsoft recommends disabling SMB 1.0 in modern networks

However, for legacy Windows XP and early Vista systems, SMB 1.0 is the only option.

Why Other Options Are Incorrect:

A . SMB V3.1.1- This is the latest version, introduced with Windows Server 2016 and Windows 10; not supported on XP or Vista

C . SMB is not required for XP or Vista- Incorrect; SMB is essential for Windows manageability and script execution

D . SMB V2.0- While Vista supports SMB 2.0, Windows XP does NOT; only SMB 1.0 works on both

E . SMB V3.0- This requires Windows 8/Server 2012 or later; not supported on XP or Vista

Legacy Endpoint Management Considerations:

According to the documentation:

For legacy endpoints requiring SMB 1.0:

Cannot require SMB signing (not supported in SMB 1.0)

Must allow unencrypted SMB communication

Should be isolated on network segments with security controls

Represents security risk due to SMB 1.0 vulnerabilities

Referenced Documentation:

Forescout HPS Inspection Engine - About SMB documentation

Operational Requirements - Port requirements

Microsoft - SMB Protocol Versions and Requirements

Microsoft - Detect, Enable, and Disable SMBv1, SMBv2, and SMBv3 in Windows

Question 8

Question Type: MultipleChoice

The host property 'HTTP User Agent banner' is resolved by what function?

Options:

A- Device classification engine
B- NetFlow
C- NMAP scanning
D- Packet engine
E- Device profile library

Answer:

D

Explanation:

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

According to theForescout Administration Guide - Advanced Classification Properties, the host property'HTTP User Agent banner' is resolved by the Packet Engine.

HTTP User Agent Banner Property:

According to the Advanced Classification Properties documentation:

TheHTTP User Agentproperty is captured through passive network traffic analysis by the Packet Engine, which monitors and analyzes HTTP headers in network traffic.

Packet Engine Function:

According to the Packet Engine documentation:

The Packet Engine provides:

Passive Traffic Monitoring- Analyzes network packets without interfering

HTTP Header Analysis- Extracts HTTP headers from captured traffic

User Agent Detection- Identifies HTTP User Agent strings from web requests

Property Resolution- Populates device properties from observed traffic

HTTP User Agent Examples:

Common User Agent banners that identify device types and browsers:

text

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36

Mozilla/5.0 (iPhone; CPU iPhone OS 14_6 like Mac OS X) AppleWebKit/605.1.15

Mozilla/5.0 (Linux; Android 11; SM-G991B) AppleWebKit/537.36

Why Other Options Are Incorrect:

A . Device classification engine- The classification engine uses properties resolved by other components like the Packet Engine

B . NetFlow- NetFlow provides flow statistics, not application-level data like HTTP headers

C . NMAP scanning- NMAP performs active port scanning, not passive HTTP header analysis

E . Device profile library- The profile library uses properties; it doesn't resolve them

Property Resolution by Function:

According to the documentation:

Property

Packet Engine

NMAP

Device Class Engine

Profile Library

HTTP User Agent

Yes

No

No

No

Service Banner

No

Yes

No

No

OS Classification

Partial

Partial

Yes

No

Function

No

No

Yes

Yes

Referenced Documentation:

Advanced Classification Properties

About the Packet Engine

Forescout Platform Dependencies and Known Issues

Question 9

Question Type: MultipleChoice

Proper policy flow should consist of...

Options:

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 classify sub-rule should flow to an assess policy, IoT classify policies typically test manageability, IT classify usually indicates ownership.
C- 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.
D- 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.
E- 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.

Answer:

B

Explanation:

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

According to theForescout 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 indicateOWNERSHIP(corporate vs. BYOD)

Determine if device is managed or unmanaged

Establish if device belongs to organization

IoT Device Classification Policies:

Typically testMANAGEABILITY(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

Question 10

Question Type: MultipleChoice

What should be done after the Managed Windows devices are sent to a policy to determine the Windows 10 patch delivery optimization setting?

Options:

A- Push out the proper DWORD setting via GPO

B- Non Windows 10 devices must be called out in sub-rules since they will not have the relevant

DWORD

C- Manageable Windows devices are not required by this policy

D- Non Windows 10 devices must be called out in sub-rules so that the relevant DWORD value may be changed

E- Write sub-rules to check for each of the DWORD values used in patch delivery optimization

Answer:

E

Explanation:

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

After managed Windows devices are sent to a policy to determine the Windows 10 patch delivery optimization setting, the best practice is towrite sub-rules to check for each of the DWORD values used in patch delivery optimization.

Windows 10 Patch Delivery Optimization DWORD Values:

Windows 10 patch delivery optimization is configured through DWORD registry settings in the following registry path:

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeliveryOptimization

The primary DWORD value isDODownloadMode, which supports the following values:

0= HTTP only, no peering

1= HTTP blended with peering behind the same NAT (default)

2= HTTP blended with peering across a private group

3= HTTP blended with Internet peering

63= HTTP only, no peering, no use of DO cloud service

64= Bypass mode (deprecated in Windows 11)

Why Sub-Rules Are Required:

When implementing a policy to manage Windows 10 patch delivery optimization settings, administrators must createsub-rules for each possible DWORD configuration valuebecause:

Different Organizational Requirements- Different departments or network segments may require different delivery optimization modes (e.g., value 1 for some devices, value 0 for others)

Compliance Checking- Each sub-rule verifies whether a device has the correct DWORD value

configured according to organizational policy

Enforcement Actions- Once each sub-rule identifies a specific DWORD value, appropriate remediation actions can be applied (e.g., GPO deployment, messaging, notifications)

Granular Control- Sub-rules allow for precise identification of devices with non-compliant delivery optimization settings

Implementation Workflow:

Device is scanned and identified as Windows 10 managed device

Policy queries theDODownloadModeDWORD registry value

Multiple sub-rules evaluate the current DWORD value:

Sub-rule for value '0' (HTTP only)

Sub-rule for value '1' (Peering behind NAT)

Sub-rule for value '2' (Peering across private group)

Sub-rule for value '3' (Internet peering)

Sub-rule for value '63' (No peering, no cloud)

Matching sub-rule triggers appropriate policy actions

Why Other Options Are Incorrect:

A . Push out the proper DWORD setting via GPO- This is what you do AFTER checking via sub-rules, not what you do after sending devices to the policy

B . Non Windows 10 devices must be called out in sub-rules since they will not have the relevant DWORD- While non-Windows 10 devices should be excluded, the answer doesn't address the core requirement of checking each DWORD value

C . Manageable Windows devices are not required by this policy- This is incorrect; managed Windows devices are the focus of this policy

D . Non Windows 10 devices must be called out in sub-rules so that the relevant DWORD value may be changed- This misses the point; you check the DWORD values first, not change them in sub-rules

Referenced Documentation:

Microsoft Delivery Optimization Reference - Windows 10 Deployment

Forescout Administration Guide - Defining Policy Sub-Rules

How to use Group Policy to configure Windows Update Delivery Optimization

Question 11

Question Type: MultipleChoice

Which option best requires secure connector to resolve?

Options:

A- Authentication login (advanced)
B- Authentication certificate status
C- HTTP login user
D- Authentication login
E- Signed-In status

Answer:

D

Explanation:

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

According to theForescout HPS Inspection Engine Configuration Guide and Remote Inspection Feature Support documentation,'Authentication login' requires SecureConnector to resolve.

Authentication Login Property:

According to the Remote Inspection and SecureConnector Feature Support documentation:

The'Authentication login'property requires SecureConnector because:

Interactive User Information- Requires access to active user session data

Real-Time Verification- Must check current login status

Endpoint Agent Needed- Cannot be determined via passive network monitoring or remote registry

SecureConnector Required- Installed agent must report login status

SecureConnector vs. Remote Inspection:

According to the HPS Inspection Engine guide:

Some properties require different capabilities:

Property

Remote Inspection (MS-WMI/RPC)

SecureConnector

Authentication login

No

Yes

Authentication login (advanced)

No

Yes

Signed-In status

No

Yes

HTTP login user

No

Yes

Authentication certificate status

Yes

Yes

Why Other Options Are Incorrect:

A . Authentication login (advanced)- While this also requires SecureConnector, the base 'Authentication login' is the more accurate answer

B . Authentication certificate status- This can be resolved via Remote Inspection using certificate stores

C . HTTP login user- This is resolved by SecureConnector, but not listed as requiring it in the same way

E . Signed-In status- While this requires SecureConnector, the more specific answer is 'Authentication login'

SecureConnector Capabilities:

According to the documentation:

SecureConnector resolves endpoint properties that require:

Active user session information

Real-time application/browser monitoring

Deep endpoint inspection

Interactive user credentials

Referenced Documentation:

Remote Inspection and SecureConnector -- Feature Support

Using Certificates to Authenticate the SecureConnector Connection

P2P exams