



Forescout FSCP Practice Questions

Shared by Livingston on 08-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

Based on ForeScout's recommended troubleshooting approach, where should you start the troubleshooting process?

Options:

- A- Run fstool tech-support
- B- Check that requirements are met
- C- Look at dependencies
- D- Examine the GUI Logs
- E- Review command line logs

Answer:

B

Explanation:

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

According to theForeScout troubleshooting methodology, the recommended starting point for the troubleshooting process is to'Check that requirements are met'. This foundational step must come before any detailed investigation.

ForeScout Troubleshooting Approach:

The basic troubleshooting workflow consists of:

text

Step 1: CHECK THAT REQUIREMENTS ARE MET (START HERE)

System requirements

Software versions

Network connectivity

Licensing

Step 2: Look at Dependencies

Network dependencies

Service dependencies

Appliance dependencies

Step 3: Gather Information from CounterACT

GUI logs

Properties

Policies

Step 4: Gather Information from Command Line

CLI logs

Network diagnostics

Step 5: Form Hypothesis and Diagnose

Analyze findings

Determine root cause

Why Checking Requirements is the First Step:

According to the troubleshooting best practices:

Foundation- Verifying requirements prevents wasting time on invalid configurations

System Integrity- Ensures all prerequisites are met before investigating issues

Efficiency- Many issues stem from unmet requirements; fixing these resolves the problem immediately

Logical Flow- Without meeting requirements, no further troubleshooting will be effective

Why Other Options Are Incorrect:

A . Run fstool tech-support- This is an advanced diagnostic tool, not the starting point

C . Look at dependencies- Dependencies are examined AFTER confirming requirements are met

D . Examine the GUI Logs- Logs are reviewed AFTER requirements and dependencies are checked

E . Review command line logs- CLI logs are examined later in the process, not first

Requirements Verification Includes:

According to the methodology:

System Requirements

Supported OS versions

Memory and storage requirements

CPU specifications

Software Versions

Forescout platform version

Plugin/module compatibility

Browser versions for Console

Network Connectivity

IP address configuration

Network interfaces

Firewall rules

Licensing

Valid licenses

License not expired

License for required modules

Referenced Documentation:

Basic troubleshooting approach methodology

Question 2

Question Type: MultipleChoice

Which of the following is a User Directory feature?

Options:

A- Guest authentication

B- Dashboard

C- Radius authorization

D- Query Switches

E- Assets portal

E- Assets portal- This is a general Forescout platform feature, not specific to the User Directory plugin

Authentication Module Structure:

According to the documentation, the Authentication Module consists of two plugins:

RADIUS Plugin- Handles 802.1X authentication, authorization, and accounting

User Directory Plugin- Handles user resolution, authentication, and guest management

These work together but have distinct responsibilities. The User Directory Plugin specifically handles guest authentication among its feature set.

Referenced Documentation:

Forescout Authentication Module Overview Guide Version 1.1

About the User Directory Plugin documentation

User Directory Plugin Server and Guest Management Configuration Guide

Answer:

A

Explanation:

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

Guest authentication is a User Directory feature. According to the Forescout Authentication Module Overview Guide and the User Directory Plugin Configuration Guide, the User Directory Plugin enables guest authentication and management through configured directory servers.

User Directory Plugin Features:

The User Directory Plugin (version 6.4+) provides the following core features:

Endpoint User Resolution- Resolves endpoint user details by querying directory servers

User Authentication- Performs user authentication via configured internal and external directory servers (Active Directory, LDAP, etc.)

Guest Authentication- Enables authentication and registration of guest users on the network

Guest Sponsorship- Allows corporate employee sponsors to approve guest network access

Guest Management Portal- Provides functionality for managing guest hosts and guest portal access

Directory Server Integration- Integrates with enterprise directory servers for credential validation

Guest Management Capabilities:

The User Directory Plugin specifically enables:

Guest user registration and authentication

Guest approval workflows through sponsor groups

Guest session management

Guest password policies

Guest tag management for categorization

Why Other Options Are Incorrect:

B . Dashboard- This is a general console feature, not specific to the User Directory plugin

C . Radius authorization- This is the function of theRADIUS plugin, not the User Directory plugin (though they work together in the Authentication Module)

D . Query Switches- This is a function of theSwitch plugin, not the User Directory plugin

Question 3

Question Type: MultipleChoice

When configuring policies, which of the following statements is true regarding the indicated property?

Select one:

Options:

- A- Irresolvable hosts would match the condition
- B- Negates the criteria inside the property
- C- Negates the criteria outside the property
- D- Modifies the irresolvable condition to TRUE
- E- Negates the 'evaluate irresolvable as' setting

Answer:

B

Explanation:

Based on the policy condition image provided showing the NOT checkbox on 'Windows Antivirus Update Data', the correct statement is that the NOT operator negates the criteria inside the property.

Understanding the NOT Operator:

When the NOT checkbox is selected on a policy condition property, it performs logical negation (NOT operation) on the criteria evaluation. According to the ForeScout Administration Guide:

The NOT operator creates an inverted evaluation:

Without NOT: 'Windows Antivirus Update Data = [value]'

Result: Matches endpoints where the property equals the specified value

With NOT (as shown in the image): 'NOT (Windows Antivirus Update Data = [value])'

Result: Matches endpoints where the property does NOT equal the specified value

How the NOT Operator Works:

The NOT operator negates the criteria inside the property:

Criteria Evaluation- The property condition is evaluated normally first

Negation Applied- The result is then inverted (TRUE becomes FALSE, FALSE becomes TRUE)

Final Result- The endpoint matches only if the negated condition is true

Example from the Image:

The image shows:

First criterion: 'Windows Antivirus Running - 360 Sat' (AND)

Second criterion: 'NOT Windows Antivirus Update Data' (checked)

This means:

The endpoint must have Windows Antivirus Running = True (360 Sat)

AND the endpoint must NOT have the Windows Antivirus Update Data property value (whatever was specified)

The NOT negates the criteria inside the property condition

NOT vs. 'Evaluate Irresolvable As':

According to the documentation, these are independent settings:

Setting

Purpose

NOT Checkbox

Negates the criteria evaluation (inverts the match logic)

Evaluate Irresolvable As

Defines how to handle unresolvable properties (when data cannot be determined)

The NOT operator works inside the property evaluation, while 'Evaluate Irresolvable As' is a separate setting that determines behavior when a property cannot be resolved.

Why Other Options Are Incorrect:

A . Irresolvable hosts would match the condition- The NOT operator doesn't specifically affect how irresolvable properties are handled

C . Negates the criteria outside the property- The NOT operator is internal to the property; it negates the criteria inside, not outside

D . Modifies the irresolvable condition to TRUE- The NOT operator doesn't modify the 'Evaluate Irresolvable As' setting; these are independent

E . Negates the 'evaluate irresolvable as' setting- The NOT operator and 'Evaluate Irresolvable As' are separate; NOT doesn't affect or negate that setting

Policy Condition Structure:

According to the Forescout Administration Guide:

A policy condition is structured as:

text

[NOT] [Property Name] [Operator] [Value]

Where:

[NOT]- Optional negation operator (what the checkbox controls)

[Property Name]- The property being evaluated

[Operator]- The comparison operator (equals, contains, greater than, etc.)

[Value]- The value to match against

When NOT is checked, it negates the entire criteria evaluation inside that property condition.

Referenced Documentation:

Forescout Administration Guide v8.3

Forescout Administration Guide v8.4

Define policy scope documentation

Forescout eyeSight policy sub-rule advanced options

Question 4

Question Type: MultipleChoice

What is the automated safety feature to prevent network wide outages/blocks?

Options:

- A- Stop all policies
- B- Disable policy
- C- Disable Policy Action
- D- Action Thresholds
- E- Send an Email Alert

Answer:

D

Explanation:

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

Action Thresholds is the automated safety feature designed to prevent network-wide outages and blocks. According to the Forescout Platform Administration Guide, Action Thresholds are specifically designed to automatically implement safeguards when rolling out sanctions (blocking actions) across your network.

Purpose of Action Thresholds:

Action thresholds work as an automated circuit breaker mechanism that prevents catastrophic network-wide outages. The feature establishes maximum percentage limits for specific action types on a single appliance. When these limits are reached, the policy automatically stops executing further blocking actions to prevent mass network disruption.

How Action Thresholds Prevent Outages:

Consider a scenario where a policy is misconfigured and would block 90% of all endpoints on the network due to a false condition match. Without Action Thresholds, this could cause a network-wide outage. With Action Thresholds configured:

Limit Definition- An administrator sets an action threshold (e.g., 20% of endpoints can be blocked by Switch action type)

Automatic Enforcement- When this percentage threshold is reached, the policy automatically stops executing the blocking action for any additional endpoints

Alert Generation- The system generates alerts to notify administrators when a threshold has been reached

Protection- This prevents the policy from cascading failures that could affect the entire network

Action Threshold Configuration:

Each action type (e.g., Switch blocking, Port blocking, External port blocking) can be configured with its own threshold percentage. This allows granular control over the maximum impact any single policy can have on the network.

Why Other Options Are Incorrect:

A . Stop all policies- This is a manual intervention, not an automated safety feature; also, it's too drastic and would disable legitimate policies

B . Disable policy- This is a manual action, not an automated safety mechanism

C . Disable Policy Action- While you can disable individual actions, this is not an automated threshold-based safeguard

E . Send an Email Alert- Alerts notify administrators but do not automatically prevent outages; they require manual intervention

Referenced Documentation:

Forescout Platform Administration Guide - Working with Action Thresholds

Forescout Platform Administration Guide - Policy Safety Features

Section: 'Action Thresholds are designed to automatically implement safeguards when rolling out such sanctions across your network'

Question 5

Question Type: MultipleChoice

Based on ForeScout's recommended troubleshooting approach, where should you start the troubleshooting process?

Options:

- A- Run fstool tech-support
- B- Check that requirements are met
- C- Look at dependencies
- D- Examine the GUI Logs
- E- Review command line logs

Answer:

B

Explanation:

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

According to the Forescout troubleshooting methodology, the recommended starting point for the troubleshooting process is to 'Check that requirements are met'. This foundational step must come before any detailed investigation.

Forescout Troubleshooting Approach:

The basic troubleshooting workflow consists of:

text

Step 1: CHECK THAT REQUIREMENTS ARE MET (START HERE)

System requirements

Software versions

Network connectivity

Licensing

Step 2: Look at Dependencies

Network dependencies

Service dependencies

Appliance dependencies

Step 3: Gather Information from CounterACT

GUI logs

Properties

Policies

Step 4: Gather Information from Command Line

CLI logs

Network diagnostics

Step 5: Form Hypothesis and Diagnose

Analyze findings

Determine root cause

Why Checking Requirements is the First Step:

According to the troubleshooting best practices:

Foundation- Verifying requirements prevents wasting time on invalid configurations

System Integrity- Ensures all prerequisites are met before investigating issues

Efficiency- Many issues stem from unmet requirements; fixing these resolves the problem immediately

Logical Flow- Without meeting requirements, no further troubleshooting will be effective

Why Other Options Are Incorrect:

A . Run fstool tech-support- This is an advanced diagnostic tool, not the starting point

C . Look at dependencies- Dependencies are examined AFTER confirming requirements are met

D . Examine the GUI Logs- Logs are reviewed AFTER requirements and dependencies are checked

E . Review command line logs- CLI logs are examined later in the process, not first

Requirements Verification Includes:

According to the methodology:

System Requirements

Supported OS versions

Memory and storage requirements

CPU specifications

Software Versions

Forescout platform version

Plugin/module compatibility

Browser versions for Console

Network Connectivity

IP address configuration

Network interfaces

Firewall rules

Licensing

Valid licenses

License not expired

License for required modules

Referenced Documentation:

Basic troubleshooting approach methodology



Question 6

Question Type: MultipleChoice

How can scripts be run when the Endpoint Remote Inspection method is set to "Using MS-WMI"?

Options:

- A- Using Task Scheduler but this has limitations
- B- Using WMI, which will allow interactive scripts to run
- C- Using RRP, which will allow interactive scripts to run
- D- Using WMI, but they may not be run interactively using this method
- E- Using fsprocserv.exe, but scripts may not be run interactively using this method

Answer:

D

Explanation:

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

According to the Forescout CounterACT HPS Inspection Engine Configuration Guide Version 10.8, when the Endpoint Remote Inspection method is set to 'Using MS-WMI,' scripts are run using WMI, but they may not be run interactively using this method.

MS-WMI Script Execution:

According to the HPS Inspection Engine guide:

'When Remote Inspection uses MS-WMI, run scripts with

MS-WMI-- note that interactive scripts are not supported by WMI on all Windows endpoints. Functionality that relies on interactive endpoint scripts is not implemented when you choose this option. For example, the Start Antivirus and Update Antivirus actions require interactive scripts to manage some antivirus packages.'

Interactive Script Limitations with WMI:

According to the documentation:

'WMI does not support interactive scripts (such as scripts that support Guest Registration and other HTTP-based actions) on some Windows endpoints.'

How WMI Scripts Are Run:

According to the documentation:

When using WMI for script execution:

Background Scripts- Most background scripts can run via WMI

Interactive Scripts- NOT supported by WMI on all endpoints

Workaround for Interactive Scripts- CounterACT uses:

fsprocsvc service(fsprocsvc.exe) - For interactive script support

Microsoft Task Scheduler- Alternative for interactive scripts

WMI vs. Other Methods:

According to the documentation:

Method

Interactive Scripts

Limitations

MS-WMI

Not supported on all endpoints

Limited to background scripts

fsprocsvc

Supported

Service must be running

Task Scheduler

Not on Vista/7

Legacy OS limitations

Script Execution Flow with MS-WMI:

According to the documentation:

'CounterACT runs most background scripts using WMI. WMI does not support interactive scripts (such as scripts that support Guest Registration and other HTTP-based actions) on some Windows endpoints. CounterACT uses the fsprocsvc service or Microsoft Task Scheduler to run interactive scripts on these endpoints.'

Why Other Options Are Incorrect:

A . Using Task Scheduler but with limitations- Task Scheduler is an ALTERNATIVE to WMI, not what MS-WMI uses

B . Using WMI, which will allow interactive scripts- Incorrect; WMI does NOT allow interactive scripts

C . Using RRP, which will allow interactive scripts- RRP is Remote Registry Protocol, not the script execution method with MS-WMI

E . Using fsprocserv.exe, but scripts may not be run interactively- fsprocserv.exe (fsprocsvc) DOES support interactive scripts; it's used as an alternative to overcome WMI limitations

Referenced Documentation:

CounterACT Endpoint Module HPS Inspection Engine Configuration Guide v10.8 - Script Execution Services section

When Remote Inspection uses MS-WMI, run scripts with

About MS-WMI

Question 7

Question Type: MultipleChoice

Which of the following logs are available from the GUI?

Options:

- A- Host Details, Policy, Blocking, Event Viewer, Audit Trail
- B- Switch, Policy, Blocking, Event Viewer, Audit Trail
- C- Switch, Discovery, Threat Protection, Event Viewer, Audit Trail
- D- HPS, Policy, Threat Protection, Event Viewer, Audit Trail
- E- Host Details, Policy, Today Log, Threat Event Viewer, Audit Trail

Answer:

A

Explanation:

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

According to the Forescout Platform Administration Guide, the logs available from the GUI Console include: Host Details, Policy, Blocking, Event Viewer, and Audit Trail.

Available Logs from the Forescout Console GUI:

Host Details Log- Provides detailed information about individual endpoints discovered on the network. This log displays comprehensive host properties and status information directly accessible from the console.

Policy Log- Shows policy activity and records how specific endpoints are handled by policies. The Policy Log investigates endpoint activity, displaying information about policy matches, actions executed, and policy evaluation results.

Blocking Log- Displays all blocking events that occur on the network, including port blocks, host blocks, and external port blocks. This log provides an at-a-glance display of blocked endpoints with timestamps and reasons.

Event Viewer- A system log that displays severity, date, status, element, and event information. Administrators can search, export, and filter events using the Event Viewer.

Audit Trail- Records administrative actions and changes made to the Forescout platform configuration and policies.

How to Access Logs from the GUI:

From the Forescout Console GUI, administrators access logs through the Log menu by selecting:

Blocking Logs to view block events

Event Viewer to display system events

Policy Reports to investigate policy activity

Why Other Options Are Incorrect:

- B . Switch, Policy, Blocking, Event Viewer, Audit Trail- 'Switch' is not a standalone log type available from the GUI; switch data is captured through plugin logs and reports
- C . Switch, Discovery, Threat Protection, Event Viewer, Audit Trail- 'Discovery' and 'Threat Protection' are report categories, not GUI logs in the standard log menu
- D . HPS, Policy, Threat Protection, Event Viewer, Audit Trail- HPS logs are accessed through CLI, not the GUI; 'Threat Protection' is a report, not a GUI log
- E . Host Details, Policy, Today Log, Threat Event Viewer, Audit Trail- 'Today Log' and 'Threat Event Viewer' are not standard log names in the Forescout GUI

Referenced Documentation:

Forescout Platform Administration Guide - Generating Reports and Logs

Policy Reports and Logs section

Work with System Event Logs documentation

View Block Events documentation

Question 8

Question Type: MultipleChoice

When using the "Assign to VLAN action," why might it be useful to have a policy to record the original VLAN?

Choose one:

Options:

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

Answer:

D

Explanation:

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.

Question 9

Question Type: MultipleChoice

Which of the following actions can be performed with Remote Inspection?

Options:

- A- Set Registry Key, Disable dual homing
- B- Send Balloon Notification, Send email to user
- C- Disable External Device, Start Windows Updates
- D- Start Secure Connector, Attempt to open a browser at the endpoint

E- Endpoint Address ACL, Assign to VLAN

Answer:

D

Explanation:

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

According to the Forescout HPS Inspection Engine Configuration Guide Version 10.8 and the Remote Inspection and SecureConnector Feature Support documentation, the actions that can be performed with Remote Inspection include 'Start Secure Connector' and 'Attempt to open a browser at the endpoint'.

Remote Inspection Capabilities:

According to the documentation, Remote Inspection uses WMI and other standard domain/host management protocols to query the endpoint, and to run scripts and implement remediation actions on the endpoint. Remote Inspection is agentless and does not install any applications on the endpoint.

Actions Supported by Remote Inspection:

According to the HPS Inspection Engine Configuration Guide:

The Remote Inspection Feature Support table lists numerous actions that are supported by Remote Inspection, including:

Set Registry Key- Supported by Remote Inspection

Start SecureConnector- Supported by Remote Inspection

Attempt to Open Browser- Supported by Remote Inspection

Send Balloon Notification- Supported (requires SecureConnector; can also be used with Remote Inspection)

Start Windows Updates- Supported by Remote Inspection

Send Email to User- Supported action

However, the question asks which actions appear together in one option, and Option D correctly combines two legitimate Remote Inspection actions: 'Start Secure Connector' and 'Attempt to open a browser at the endpoint'.

Start SecureConnector Action:

According to the documentation:

'Start SecureConnector installs SecureConnector on the endpoint, enabling future management via SecureConnector'

This is a supported Remote Inspection action that can deploy SecureConnector to endpoints.

Attempt to Open Browser Action:

According to the HPS Inspection Engine guide:

'Opening a browser window' is a supported Remote Inspection action

However, there are limitations documented:

'Opening a browser window does not work on Windows Vista and Windows 7 if the HPS remote inspection is configured to work as a Scheduled Task'

'When redirected with this option checked, the browser does not open automatically and relies on the packet engine seeing this traffic'

Why Other Options Are Incorrect:

A . Set Registry Key, Disable dual homing- While Set Registry Key is supported, 'Disable dual homing' is not a standard Remote Inspection action

B . Send Balloon Notification, Send email to user- Both are notification actions, but the question seeks Remote Inspection-specific endpoint actions; these are general notification actions not specific to Remote Inspection

C . Disable External Device, Start Windows Updates- While Start Windows Updates is supported by Remote Inspection, 'Disable External Device' is not a Remote Inspection action; it's a network device action

E . Endpoint Address ACL, Assign to VLAN- These are Switch plugin actions, not Remote Inspection actions; they work on network device level, not endpoint level

Remote Inspection vs. SecureConnector vs. Switch Actions:

According to the documentation:

Remote Inspection Actions(on endpoints):

Set Registry Key on Windows

Start Windows Updates

Start Antivirus

Update Antivirus

Attempt to open browser at endpoint

Start SecureConnector (to deploy SecureConnector)

Switch Actions(on network devices):

Endpoint Address ACL

Access Port ACL

Assign to VLAN

Switch Block

Referenced Documentation:

Forescout CounterACT Endpoint Module HPS Inspection Engine Configuration Guide Version 10.8

Remote Inspection and SecureConnector -- Feature Support documentation

Set Registry Key on Windows action documentation

Start Windows Updates action documentation

Send Balloon Notification documentation

Question 10

Question Type: MultipleChoice

What best defines a 'Post-Connect Methodology'?

Options:

- A- 802.1X is a flavor of Post-Connect
- B- Guilty until proven innocent
- C- Innocent until proven guilty
- D- Used subsequent to pre-connect
- E- Assessed for critical compliance before IP address is assigned

Answer:

C

Explanation:

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

According to the Forescout Blog on Post-Connect Access Controls and the Comply-to-Connect framework documentation, a Post-Connect Methodology is best defined as treating endpoints as 'Innocent until proven guilty'.

Definition of Post-Connect Methodology:

According to the official documentation:

'Post-connect' is described as treating endpoints as innocent until they are proven guilty. They can connect to the network, during and after which they are assessed for acceptance criteria.'

How Post-Connect Works:

According to the Post-Connect Access Controls blog:

Initial Connection- Endpoints are allowed to connect to the network immediately (innocent)

Assessment During/After Connection- After connecting, endpoints are assessed for acceptance criteria

Compliance Checking- Endpoints are checked for:

Corporate asset status (must be company-owned)

Security compliance (antivirus, patches, encryption, etc.)

Remediation or Quarantine- Based on assessment results:

Compliant endpoints: Full access

Non-compliant endpoints: Placed in quarantine for remediation

Post-Connect vs. Pre-Connect:

According to the Comply-to-Connect documentation:

Pre-Connect- 'Guilty until proven innocent' - Endpoint must prove compliance BEFORE getting network access

Post-Connect- 'Innocent until proven guilty' - Endpoint connects first, then compliance is assessed

Benefits of Post-Connect Methodology:

According to the documentation:

'The greatest benefit to the post-connect approach is a positive user experience. Unless a system is out of compliance and ends up in a quarantine, your company's users have no idea access controls are even taking place on the network.'

Acceptance Criteria in Post-Connect:

According to the framework:

Corporate Asset Verification- Determines if the endpoint belongs to the organization

Compliance Assessment- Checks for:

Updated antivirus

Patch levels

Disk encryption status

Security tool functionality

If an endpoint fails these criteria, it's placed in quarantine (controlled network access) rather than being completely blocked.

Why Other Options Are Incorrect:

A . 802.1X is a flavor of Post-Connect- 802.1X is a pre-connect access control method (requires authentication before network access)

B . Guilty until proven innocent- This describes pre-connect methodology, not post-connect

D . Used subsequent to pre-connect- While post-connect can follow pre-connect, this doesn't define what post-connect is

E . Assessed for critical compliance before IP address is assigned- This describes pre-connect methodology

Referenced Documentation:

Forescout Blog - Post-Connect Access Controls

Comply-to-Connect Brief - Pre-connect vs Post-connect comparison

Achieving Comply-to-Connect Requirements with Forescout

Question 11

Question Type: MultipleChoice

Which of the following are endpoint attributes learned from the Switch plugin?

Options:

A- Host Name, Mac table, Switch IP, Port Description, Host Table, Switch Version

B- Port VLAN, Switch Version, Mac address, Host name, Port Description, ARP Table, Switch Version

C- Mac address, Host name, Port VLAN, Port Description, Switch OS, Switch Version

D- Switch Version, Mac address, Switch OS, Port VLAN, Host Name, ARP Table

E- Mac address, Switch IP and Port name, ARP Table, Switch Port Information

Answer:

C

Explanation:

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

According to the Forescout Switch Plugin documentation and Switch Properties, the endpoint attributes learned from the Switch plugin are: Mac address, Host name, Port VLAN, Port Description, Switch OS, and Switch Version.

Switch Plugin Endpoint Properties:

According to the Switch Properties documentation:

The Switch plugin learns and populates the following endpoint attributes:

Mac address- MAC address of the endpoint

Host name- Device hostname from switch ARP table

Port VLAN- VLAN ID assigned to the switch port

Port Description- Switch port alias/description

Switch OS- Operating system of the switch

Switch Version- Software version of the switch

Why Other Options Are Incorrect:

A . Includes 'Mac table' and 'Host Table'- These are switch resources, not endpoint attributes

B . Lists 'ARP Table' and duplicates 'Switch Version'- ARP table is not an endpoint attribute

D . Includes 'ARP Table'- ARP table is a switch resource, not an endpoint attribute

**E. 'Switch IP and Port name' - 'Switch IP' is not an endpoint attribute; should be 'Port VLAN'

Distinction: Switch Resources vs. Endpoint Attributes:

According to the documentation:

Endpoint Attributes(learned about the endpoint):

Mac address

Host name

Port VLAN

Port Description

Switch OS

Switch Version

Switch Resources(infrastructure information):

Mac table

ARP table

Host table

Referenced Documentation:

Switch Properties - v8.4.4

Switch Properties - v8.16.h

Switch Properties - v8.1.x



Question 12

Question Type: MultipleChoice

Which option best is the best way to brand the CounterACT HTTP pages to look like corporate internal web pages?

Options:

- A- Using the 'Reports Portal,' modify the CSS for the desired skins
- B- This is not possible with CounterACT portal and HTTP pages
- C- Using the 'User Portal Builder,' modify the CSS for the desired skins
- D- Have a webmaster modify the HTML pages within the Tomcat web server
- E- Using the 'User Portal Builder' basic interface

Answer:

C

Explanation:

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

According to the Forescout Administration Guide, the best way to brand CounterACT HTTP pages to match corporate identity is to use the 'User Portal Builder' to modify the CSS for the desired skins'. This is the officially supported method for customizing the appearance of Forescout portal pages.

User Portal Builder for Branding:

The User Portal Builder provides:

CSS Customization- Modify cascading stylesheets to match corporate branding

Skin Selection- Choose different portal skins/themes

Logo and Colors- Customize logos, color schemes

Supported Customization- Official, supported method through the GUI

Why Option C is Correct:

The User Portal Builder specifically provides CSS modification capabilities to customize the appearance of Forescout HTTP portal pages to match organizational branding standards.

Why Other Options Are Incorrect:

A . Reports Portal- Reports Portal is separate from HTTP portal pages; not for branding

B . Not possible- Customization IS possible through User Portal Builder

D . Modify HTML in Tomcat- While technically possible, this is NOT supported; may break with updates

E . Basic interface only- The full User Portal Builder supports CSS modification, not just basic interface

Supported Customization Methods:

According to the documentation:

User Portal Builder (CSS)- Supported, recommended method

Direct Tomcat HTML modification- Not supported; unsupported method

Manual CSS editing- Unsupported; may conflict with updates

Referenced Documentation:

Forescout Administration Guide - User Portal Builder section

Question 13

Question Type: MultipleChoice

Which of the following is a characteristic of a centralized deployment?

Options:

- A- Checking Microsoft vulnerabilities at remote site may have significant bandwidth impact
- B- Provides enhanced IPS and HTTP actions
- C- Is optimal for threat protection
- D- Deployed as a Layer-2 channel
- E- Every site has an appliance

Answer:

A

Explanation:

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

According to the Forescout Installation Guide and Windows Vulnerability DB Configuration Guide, a characteristic of a centralized deployment is that checking Microsoft vulnerabilities at a remote site may have significant bandwidth impact.

Centralized vs. Distributed Deployment Models:

In a centralized deployment, Forescout uses a central location with Enterprise Manager and Appliances, while in a distributed deployment, appliances are placed at multiple locations.

Bandwidth Considerations in Centralized Deployments:

According to the Windows Vulnerability DB Configuration Guide:

'Minimize Bandwidth During Vulnerability File Download: You can minimize bandwidth usage during Microsoft vulnerability file download processes by limiting the number of concurrent HTTP downloads to endpoints. The default is 20 endpoints simultaneously.'

The documentation further states:

'To customize: Select Tools>Options>HPS Inspection Engine>Windows Updates tab. Define a value in the Maximum Concurrent Vulnerability DB File HTTP Uploads field.'

This configuration option exists specifically because checking Microsoft vulnerabilities (downloading vulnerability definition files to endpoints and having endpoints

upload compliance data back) can consume significant bandwidth.

Why Centralized Deployments Magnify Bandwidth Impact:

According to the Installation Guide:

In a centralized deployment:

All vulnerability checking traffic flows through a single central location

Multiple endpoints simultaneously download large vulnerability database files

All endpoints upload vulnerability compliance data back to central appliances

All this traffic concentrates at the central site

In contrast, in a distributed deployment where appliances exist at remote sites, local endpoints can communicate directly with the local appliance without impacting the central WAN link.

Bandwidth Management for Centralized Deployments:

According to the documentation:

To address the bandwidth impact in centralized deployments:

Limit concurrent HTTP uploads for vulnerability DB files

Schedule vulnerability checks during off-peak hours

Carefully plan deployment architecture considering remote site bandwidth

Why Other Options Are Incorrect:

B . Provides enhanced IPS and HTTP actions- This is not specific to centralized deployments; both deployment models can use IPS and HTTP actions

C . Is optimal for threat protection- Neither deployment model is necessarily optimal; choice depends on specific requirements

D . Deployed as a Layer-2 channel- Deployment mode (Layer-2 vs. Layer-3) is independent of centralized vs. distributed architecture

E . Every site has an appliance- This describes a distributed deployment, not a centralized one. In centralized deployments, appliances are concentrated at a central site

Centralized Deployment Characteristics:

According to the documentation:

Appliances are typically located at a central site

Remote sites connect through WAN links

Reduced operational complexity with centralized management

Higher bandwidth requirements on WAN for vulnerability checking and policy enforcement

Requires careful bandwidth planning for remote vulnerability assessment

Referenced Documentation:

Forescout Platform Installation Guide - Network Deployment Requirements

Windows Vulnerability DB Configuration Guide - Minimize Bandwidth During Vulnerability File Download

Forescout Platform Cloud Strategies and Best Practices - Bandwidth considerations



To Get Premium Files for FSCP Visit

<https://www.p2pexams.com/products/fscp>

For More Free Questions Visit

<https://www.p2pexams.com/forescout/pdf/fscp>

20%
DISCOUNT

P2P
exams