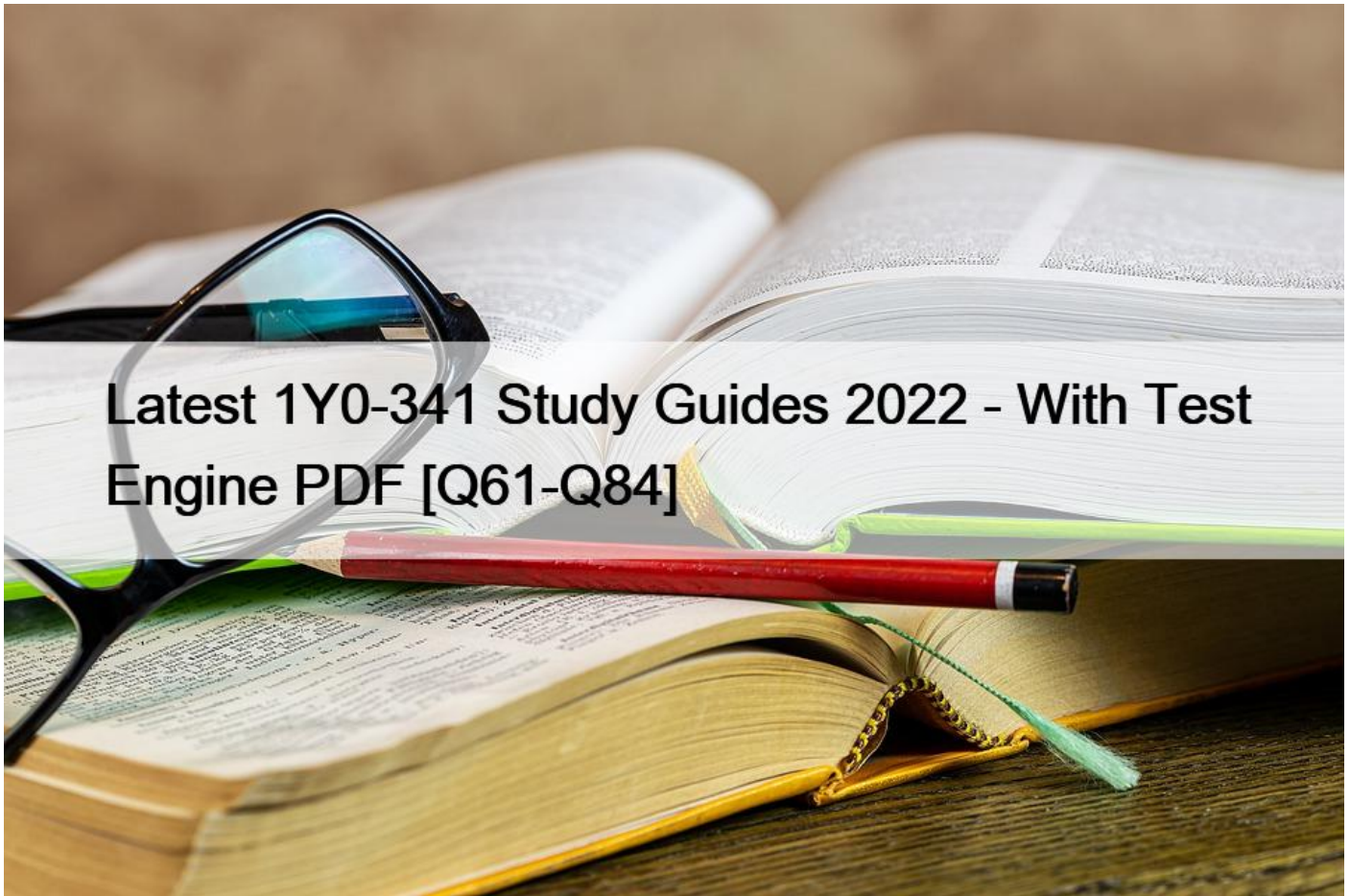


Latest 1Y0-341 Study Guides 2022 - With Test Engine PDF [Q61-Q84]



Latest 1Y0-341 Study Guides 2022 - With Test Engine PDF [Q61-Q84]

Latest 1Y0-341 Study Guides 2022 - With Test Engine PDF
Get New 1Y0-341 Practice Test Questions Answers

NO.61 A Citrix Engineer needs to ensure that infrastructure is PCI DSS compliant. Which two are prerequisite actions for PCI DSS compliance? (Choose two.)

- * Use only vendor-supplied defaults for system passwords and other security parameters.
- * Assign a unique ID to each person with computer access.
- * Track and monitor every transaction of the cardholder.
- * Regularly test security systems and processes.
- * Ensure that cardholder data is sent unencrypted over public networks.

NO.62 Which Citrix Web App Firewall profile setting can a Citrix Engineer configure to provide a response when a violation occurs?

- * Default Request
- * Redirect URL
- * Return URL
- * Default Response

Explanation/Reference: <https://docs.citrix.com/en-us/netScaler/11-1/application-firewall/profiles/configuring-profiles.html>

NO.63 Scenario: A Citrix Engineer configured an HTTP Denial-of-Service (DoS) protection policy by setting the Surge Queue depth to 300. The surge queue reaches a size of 308, triggering the NetScaler `no-attack` mode. The HTTP DoS window mechanism is left at the default size which, when reached, will trigger `no-attack` mode.

Which queue depth value must the Surge Queue be to trigger the `no-attack` mode?

- * size should be less than 280.
- * size should be 300.
- * size should be 290.
- * size should be between 280 and 300.

NO.64 Which Citrix Application Delivery Management (ADM) Analytics page allows a Citrix Engineer to monitor the metrics of the optimization techniques and congestion control strategies used in Citrix ADC appliances?

- * Gateway Insight
- * TCP Insight
- * HDX Insight
- * Web Insight

<https://docs.citrix.com/en-us/tech-zone/design/reference-architectures/citrix-adm.html>

NO.65 Which build-in TCP profile can a Citrix Engineer assign to a virtual server to improve performance for users who access an application from a remote office over an ATM connection?

- * `nstcp_default_tcp_lfp`
- * `nstcp_default_tcp_lan`
- * `nstcp_default_tcp_interactive_stream`
- * `nstcp_default_tcp_lnp`

NO.66 A Citrix Engineer has determined that users are able to access random URLs on a web site through bookmarks and by manually typing in the URLs to skip the pages required to reach that part of the website.

Which two checks can the engineer enable to prevent this attack? (Choose two.)

- * Form Field Consistency
- * Deny URL
- * Start URL
- * Buffer overflow
- * HTML Cross-site scripting

NO.67 Which Citrix Application Delivery Management (ADM) Analytics page allows an engineer to measure the ICA Round Trip Time for user connections?

- * Security Insight
- * Gateway Insight
- * TCP Insight
- * HDX Insight
- * Web Insight

NO.68 Scenario: A Citrix Engineer is monitoring the environment with Citrix Application Delivery Management (ADM). Management has asked for a report of high-risk traffic to protected internal websites.

Which dashboard can the engineer use to generate the requested report?

- * App Security
- * Transactions

- * Users & Endpoints
- * App

NO.69 Scenario: A Citrix Engineer needs to forward the Citrix Web App Firewall log entries to a central management service. This central management service uses an open log file standard.

Which log file format should the engineer use in the Citrix Web App Firewall engine settings to designate the open log file standard?

- * CEF
- * IIS
- * W3C
- * TLA

Explanation/Reference: <https://support.citrix.com/article/CTX136146>

NO.70 A Citrix Engineer has defined an HTTP Callout, hc_authorized_location, to return the value “Authorized” if client’s IP address is on a list of authorized external locations.

Which advanced expression should the engineer use in a policy for testing this condition?

- * SYS.HTTP_CALLOUT(hc_authorized_location).IS_TRUE
- * SYS.HTTP_CALLOUT(hc_authorized_location).EQ(“Authorized”)
- * SYS.HTTP_CALLOUT(hc_authorized_location).IS_VALID
- * SYS.HTTP_CALLOUT(hc_authorized_location).EQUALS_ANY(“Authorized”)

NO.71 Scenario: A Citrix Engineer wants to configure the Citrix ADC for OAuth authentication. The engineer uploads the required certificates, configure the actions, and creates all the necessary policies. After binding the authentication policy to the application, the engineer is unable to authenticate.

What is the most likely cause of this failure?

- * The log files are full.
- * The Redirect URL is incorrect.
- * The certificates have expired.
- * The policy bindings were assigned incorrect priorities.

Explanation/Reference: <https://docs.citrix.com/en-us/citrix-adc/current-release/aaa-tm/entities-of-authentication-authorization-auditing/authentication-policies.html>

NO.72 Which is a single-digit rating system that indicates the criticalness of attacks on the application, regardless of whether or NOT the application is protected by a NetScaler appliance?

- * App Store
- * Safety Index
- * Threat Index
- * Transactions

NO.73 Which data populates the Events Dashboard?

- * Syslog messages
- * SNMP trap messages
- * API calls
- * AppFlow IPFIX records

NO.74 Scenario: A Citrix Engineer has created a default admin user with username Admin1 and password `nsroot’ for the tenant example-online. However, the tenant administrator is unable to log in as username Admin1 and password `nsroot’.

Which action resolves this problem?

- * User should use the system administrator credentials to login.
- * The user BIND DN should be specified.
- * The default password must be change before login.
- * User should enter username as example-onlineAdmin1.

NO.75 Scenario: A Citrix Engineer has configured a NetScaler Management Analytics System (NMAS) policy mandating that all certificates must have minimum key strengths of 2048 bits and must be authorized by trusted CA/Issuers.

How does NMAS alert the engineer about non-compliance?

- * NMAS highlights any non-compliance with the `Non-Recommended` tag.
- * NMAS disables any non-compliant policies.
- * NMAS does NOT alert the engineer.
- * NMAS disables any non-compliant certificates.

NO.76 A company has experienced an outage of their mission-critical website. Upon investigation, the Citrix Engineer determines that the following command was executed on the website:

```
DROP TABLE table_name
```

Which security check would have prevented this issue?

- * HTML SQL Injection
- * Form Field Consistency
- * HTML Cross-Site Scripting
- * Field Formats

NO.77 Scenario: A Citrix Engineer needs to block requests from a list of IP addresses in a database maintained by the Security team. The Security team has built a web application that will send a response of either `Blocked` or `Allowed` based on whether the given IP address is on the list. Which expression should the engineer use to extract the status for policy processing?

- * HTTP.RES.CONTENT LENGTH.GT(0)
- * HTTP.RES.HEADERf Connection;))
- * HTTP.RES.STATUS
- * HTTP.RES.BODY(1000)

NO.78 Which three protocols in a NetScaler Management and Analytics System (NMAS) can be used to back up the current state of the managed NetScaler instances? (Choose three.)

- * Telnet
- * Secure Shell (SSH)
- * NITRO calls
- * HTTP
- * Secure Copy (SCP)

You can manually backup and restore NetScaler configurations using the GUI, CLI, or you can use NetScaler MAS to perform automatic backups and manual restores. NetScaler MAS backs up the current state of your managed NetScaler instances by using NITRO calls and the Secure Shell (SSH) and Secure Copy (SCP) protocols.

NO.79 A Citrix Engineer has configured SQL Injection security check to block all special characters.

Which two requests will be blocked after enabling this check? (Choose two.)

- * Citrix; Sqltest

- * 175// OR 1//=1//
- * Citrix” OR “1”=”1
- * Citrix OR 1=1
- * 175′ OR `1’=`1′

NO.80 Scenario: A Citrix Engineer configures the Application Firewall for protecting a sensitive website. The security team captures traffic between a client and the website and notes the following cookie:

citrix_ns_id

The security team is concerned that the cookie name is a risk, as it can be easily determined that the NetScaler is protecting the website.

Where can the engineer change the cookie name?

- * Application Firewall Policy
- * Application Firewall Engine Settings
- * Application Firewall Default Signatures
- * Application Firewall Profile

NO.81 Statistics for which three types of violations are presented on the App Security Dashboard? (Choose three.)

- * Web App Firewall protection
- * IP Reputation
- * SSL Enterprise Policy
- * Signature
- * AAA

Explanation/Reference: <https://docs.citrix.com/en-us/citrix-application-delivery-management-service/analytics/security/security-violations.html>

NO.82 Statistics for which three types of violations are presented on the App Security Dashboard?

(Choose three.)

- * Web App Firewall protection
- * IP Reputation
- * SSL Enterprise Policy
- * Signature
- * AAA

<https://docs.citrix.com/en-us/citrix-application-delivery-management-service/analytics/security/security-violations.html>

NO.83 What can a Citrix Engineer use in NetScaler Management and Analytics System (NMAS) to troubleshoot an issue in which users report long response times when accessing a virtual desktop?

- * Web Insight
- * WAN Insight
- * HDX Insight
- * Gateway Insight

NO.84 Which Front End Optimization technique overcomes the parallel download limitation of web browsers?

- * Domain Sharding
- * Minify

- * Extend Page Cache
- * Lazy Load

Citrix CCP-AppDS Exam Syllabus Topics: **Section Objectives** Authentication using Security Assertion Markup Language (SAML)- Determine how to configure SAML based on a given scenario. Citrix ADC Security and Filtering- Determine how to implement HTTP Callout.

- Determine how to implement IP rate-limiting.

- Determine how to implement IP reputation.

- Determine how to Implement AppQoE. Additional Citrix Web App Firewall Protections- Determine how to configure cookie consistency checks for an environment.

- Determine how to configure advanced form protection checks for an environment.

- Determine how to appropriately protect URLs based on a description of an environment.

- Determine how to appropriately protect the data based on a description of an environment. Citrix Web App Firewall Profiles and Policies- Determine how to configure Citrix Web App Firewall Policies.

- Determine how to create or implement (binding) Citrix Web App Firewall profiles.

- Determine how to configure Citrix Web App Firewall learning for a given scenario.

- Determine how to analyze Citrix Web App Firewall settings. Introducing Citrix Web App Firewall- Determine how to audit for PCI-DSS compliance.

- Determine the appropriate methodology to use for a given scenario.

- Determine the functionality of Citrix Web App Firewall, given a scenario. Authentication using OAuth and OpenID- Determine how to configure OAuth and OpenID based on a description of a Citrix ADC environment.

- Determine how to configure multi-factor authentication in a Citrix ADC environment based on a given scenario. Integrated Caching- Determine when to use static or dynamic content requests.

- Determine how to configure cache policies.

- Determine which content group settings to configure based on a given scenario. Front End Optimization- Determine how to utilize front-end optimizations based on a given scenario. Monitoring and Troubleshooting Citrix Web App Firewall- Determine how to deploy Citrix Web App Firewall for a given environment.- Determine how Citrix Web App Firewall interacts with applications in a

given environment.

- Determine how to resolve Citrix Web App Firewall configuration issues given a description of an issue.
- Determine how to Implement logging and reporting.
- Determine how to customize error pages for a given environment.
- Identify troubleshooting methods for Citrix Web App Firewall.Performance Tuning and Other Optimizations- Determine how the Citrix ADC system uses HTTP connections based on a given description.
- Determine how to Tune HTTP and TCP behaviors in Connection Profiles.Managing and Monitoring Citrix ADC Instances- Determine how to manage multiple instances in a single Citrix Application Delivery Management deployment with Instance Management.
- Determine how to manage the aspects of Authentication and Authorization on Citrix ADM.
- Identify what data is captured and utilized with Analytics and Automation.
- Determine how to configure and install SSL Certificates on Citrix Application Delivery Management.
- Determine how to monitor user connections using dashboards.Managing Citrix ADC Configurations- Determine how to manage applications in a Citrix ADC environment.
- Determine how to create, manage, and configure StyleBooks.
- Determine how to complete configuration jobs based on a scenario.

1Y0-341 Dumps and Exam Test Engine: <https://www.examcollectionpass.com/Citrix/1Y0-341-practice-exam-dumps.html>]