Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

1Y0-341 MCQs
1Y0-341 Exam Questions
1Y0-341 Practice Test
1Y0-341 TestPrep
1Y0-341 Study Guide

PASS

killexams.com

Citrix

1Y0-341

Citrix ADC Advanced Topics - Security Management and Optimization (CCP-AppDS)

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/1Y0-341

Question: 718

After modifying signature rule coverage, how should effectiveness be validated? (Select one)

A. Simulate attacks against protected endpoints and verify POLICY BLOCK events in logs
B. Lower all policy priorities
C. Review bandwidth graphs only
D. Disable all protections and monitor application uptime

Answer: A
Explanation: Simulated attack validation demonstrates actual protection and logs confirm successful enforcement, closing the loop in continuous defense.

Question: 719

An engineer modifies a StyleBook by composing several existing StyleBooks together for a multi-tier app deployment. What is this method called? (Select one)

A. Atomic config deployment
B. Composable StyleBooks
C. Imperative config
D. Dashboard templating

Answer: B
Explanation: StyleBooks are composable; you can build new ones using existing as units or "building blocks".

Question: 720

In a complex scenario for SAML configuration on NetScaler 15.0-12.45, set up SAML as IdP for a serverless application with NameID format as persistent, encrypting assertions using AES-256 with certificate "enc_cert", and audience restriction to "urn:serverless:app", while enabling logout binding to POST and configuring a relay state rule "HTTP.REQ.URL.PATH". Which CLI command creates the IdP profile? (Select one)

A. configure idp serverless persistent aes256 enc urn post urlpath
B. add authentication samlIdPProfile idp_serverless -nameIDFormat PERSISTENT -encryptAssertion ENABLE -encryptionCertName enc_cert -encryptionAlgorithm AES256 -audience "urn:serverless:app" -logoutBinding POST -relayStateRule "HTTP.REQ.URL.PATH"

C. set saml idp serverless nameid persist encrypt aes256 cert enc audience urn logout post relay urlpath
D. add samlProfile prof_serverless persistent encrypt enc_cert aes audience serverless logout post relay path

Answer: B
Explanation: The add authentication samlIdPProfile command specifies nameIDFormat PERSISTENT for consistent identifiers, encryptAssertion ENABLE with encryptionCertName and encryptionAlgorithm AES256 for secure transmission, audience restriction to urn:serverless:app, logoutBinding POST for secure logout, relayStateRule "HTTP.REQ.URL.PATH" to pass state, suitable for serverless SAML flows.

Question: 721

Which advanced configuration best protects applications from malicious XML payloads exploiting parsing or entity expansion vulnerabilities? (Select one)

A. Log all XML traffic without blocking
B. Only set buffer overflow check for XML traffic
C. Disable XML checks globally
D. Enable Deep XML Security Checks including XML Denial of Service protection

Answer: D
Explanation: Deep XML checks address sophisticated XML-specific threats, including parsing flaws and resource exhaustion.

Question: 722

Determine how to implement IP reputation in NetScaler 15.0 with custom feed import from XML and apply to specific vserver. Which commands? (Select All that Apply)

A. set iprep feed custom xml bind lb vs_custom
B. rep import xml custom bind vs
C. import ns ipReputation custom_feed.xml -format XML; bind lb vserver vs_custom -ipReputation custom_feed
D. configure iprep xml custom bind vserver

Answer: C
Explanation: Import ns ipReputation with XML format; bind to lb vserver for custom feed.

Question: 723

You are tasked with "virtual patching" a vulnerability before developers deploy a fix. Which Web App Firewall feature enables this quickest mitigation? (Select one)

A. Integrated caching
B. Create a custom security signature rule
C. Use a global responder policy
D. Rate limiting

Answer: B
Explanation: Creating a custom security signature or rule at the Web App Firewall level enables immediate mitigation without application code changes, which is the essence of virtual patching.

Question: 724

Based on a description where HTTP connections are closed prematurely due to idle timeouts, how to tune in connection profiles? (Select one)

A. Use sack in TCP profile
B. Set maxReq to unlimited
C. Increase clientIdleTimeout in HTTP profile
D. Enable Nagle in TCP profile

Answer: C
Explanation: Adjusting clientIdleTimeout extends the period before idle client connections are closed, preventing premature terminations in scenarios with sporadic activity.

Question: 725

A SAML assertion must carry both a username and an employee I**D.** Which ADC configuration is required? (Select one)

A. Enable two-factor authentication
B. Create a client certificate profile
C. Add both attributes to the SAML profile and map them to LDAP attributes
D. Switch profile to OAuth

Answer: C
Explanation: Attributes in the SAML profile are mapped from LDAP or other sources so both keys (username, employee ID) can be included in issued assertions for the downstream app.

Question: 726

Which action type will allow Citrix ADC to monitor cookie attacks but not enforce blocking, useful for testing without user disruption? (Select one)

A. stats
B. block
C. log
D. none

Answer: C
Explanation: Choosing "log" causes the Web App Firewall to record detected violations without blocking them, allowing administrators to observe violations and tune rules before changing to a stricter enforcement mode.

Question: 727

In completing configuration jobs in Citrix ADC 15.0 for a 5G network migration on 2200 CPX, create a job "5g-mig" to rebind services to new backends with SCTP endpoints, using variables from CSV "endpoints.csv", executing parallel on 100 instances with timeout 300s per instance, and logging failures to Syslog server "log.5g.com". Which commands? (Select All that Apply)

A. add config job 5g-mig -rebind SCTP -variables "endpoints.csv" -parallel 100 -timeout 300
B. set job 5g-mig -logFailures "log.5g.com" -protocol SYSLOG
C. configure job 5g rebind endpoints parallel100 timeout300 failures log syslog
D. complete mig rebind sctp var csv par100 time300 log 5g syslog

Answer: A,B
Explanation: Add config job 5g-mig rebind SCTP variables "endpoints.csv" parallel 100 timeout 300 for migration; set job logFailures "log.5g.com" protocol SYSLOG logs errors.

Question: 728

Which task is required immediately after deploying a new Citrix ADM appliance to enable monitoring and management of existing ADCs? (Select one)

A. Create a scheduled report
B. Initiate backup of ADM database
C. Discover and register ADC instances in ADM
D. Disable SSL certificate validation

Answer: C
Explanation: Without discovering and registering ADCs, ADM cannot collect data or provide management capabilities over the ADC fleet.

Question: 729

When troubleshooting intermittent application failures after Web App Firewall is enabled, which sources of information are most useful? (Select all that apply)

A. Packet traces (nstrace)
B. Application error logs
C. Syslog from ADC
D. Citrix AppFW violation logs

Answer: A,B,C,D
Explanation: Combined review gives visibility into ADC blocks, specific application failures, network context, and log aggregation.

Question: 730

In monitoring Citrix Web App Firewall for NetScaler 15.0, use stat appfw to get detailed violation counters for CBOR DoS over last day, exporting to JSON. Which command? (Select two)

A. stat appfw cbor dos full 86400 json
B. stat appfw violations -type CBOR_DOS -detail FULL -timerange 86400 -format JSON > cbor_stat.json
C. monitor cbor dos stat detail day json
D. show appfw stats -violation CBOR -time 1d -json export

Answer: B
Explanation: Stat appfw violations with type CBOR_DOS, detail FULL, timerange 86400, format JSON exports counters.

Question: 731

A government portal's URLs are frequently targeted with brute force access attempts. Which layered approach can be used with Citrix ADC? (Select all that apply)

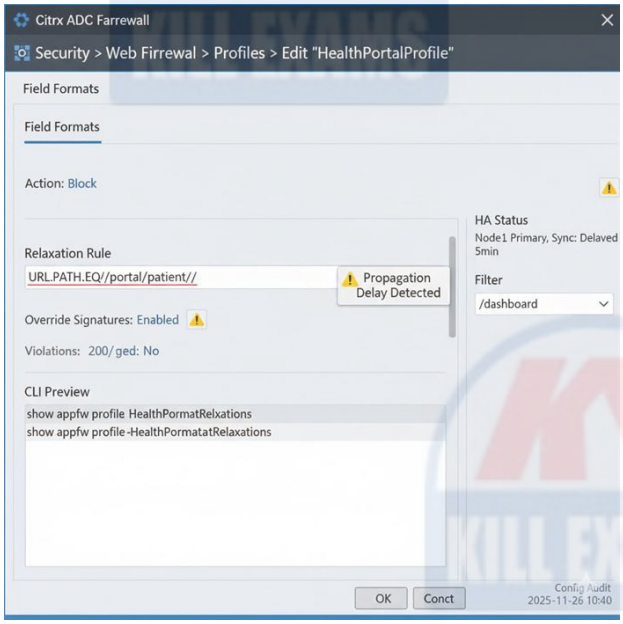
A. Add HttpOnly and Secure flags to all cookies
B. Create relaxations for trusted government IPs only

C. Enforce advanced form protection checks on sensitive submission pages
D. Enable Deny URL Checks for all restricted endpoints

Answer: A,B,C,D
Explanation: Combining restricted URL lists, strict cookie protections, IP-based relaxations, and strong form submission validation establishes layered defenses, blocking brute force as well as payload-based attacks.

Question: 732

Post-upgrade to Citrix ADC 14.1-38.53 in a healthcare portal environment, administrators report sporadic blank pages on patient dashboard loads (/portal/patient/dashboard), with Web App Firewall logs showing 200 unlogged field format violations daily despite profile bindings to cs-vserver-health. Diagnostics indicate misconfigured relaxation rules overriding signatures incorrectly, compounded by cluster propagation delays in HA pair (node1 primary). The diagram depicts the configuration issue in the profile editor.



What resolution step primarily addresses the unlogged violations and blank page renders in this HA setup?

A. Clone the profile for secondary node, apply overrides post-sync, and monitor violations via ADM reports excluding HA propagation.
B. Update the cs-vserver binding to RESP_OVERRIDE, exempt dashboard paths entirely, and defer logging to external Syslog without verbose.
C. Rebind the profile globally at REQUEST only, ignoring cluster delays, and set field formats to stats with manual relaxation per endpoint.
D. Disable signature overrides in relaxation rules, force HA sync via 'sync ha files all', and enable verbose logging for field formats to capture violations.

Answer: D

Explanation: Resolving Web App Firewall configuration issues post-upgrade, such as unlogged violations causing blank renders, stems from relaxation rules erroneously overriding signatures (e.g., field formats blocking valid patient data formats like dates), amplified by HA propagation delays in 14.1-38.53 where config pushes lag 5min on node1 primary. Disabling overrides in the relaxation rule (via profile editor > Field Formats > Edit Rule) restores signature enforcement without exemptions, ensuring violations trigger properly; executing 'sync ha files all' from CLI forces immediate cluster propagation to secondary, eliminating sync gaps; enabling verbose logging (Profile Settings > Logging > Verbose Level: High) captures detailed payloads/headers for the 200 daily events, aiding further tuning without performance hit. Global rebinds risk over-inspection, stats-only misses blocks, RESP_OVERRIDE ignores request-side issues, cloning adds management overhead—this sequenced disable-sync-enable approach swiftly restores functionality in HA healthcare environments.

Question: 733

In monitoring user connections using dashboards in Citrix ADM 14.1 for a global bank with 10000 clients, utilize Security Dashboard for WAF violations with geo-heatmaps, client fingerprint trends, and alerting on attacks >500/h via PagerDuty. Which features? (Select one)

A. Analytics Overview with Heatmap, Trends, Event webhook
B. Security Dashboard with Violation Geo-Heatmap, Fingerprint Trends, Alert Rule attacks >500/h to PagerDuty
C. Infrastructure Dashboard with Security Filter, Geo, Alerts PagerDuty
D. User Connections Dash with WAF metrics, Map, Graphs, Notification PagerDuty

Answer: B
Explanation: Security Dashboard shows violations geo-heatmap, fingerprint trends for clients, alert rule on >500/h to PagerDuty for bank security.

Question: 734

In Citrix ADC, how is a policy unbound from a virtual server using CLI? (Select one)

A. remove appfw profile <profile_name>
B. show lb vserver <vserver_name>
C. set appfw profile <profile_name> -state disabled
D. unbind appfw policy <policy_name> <vserver_name>

Answer: D
Explanation: The "unbind appfw policy" command followed by the policy and vserver names detaches the specified policy, ceasing its enforcement.

Question: 735

In a NetScaler 15.0 deployment managing Citrix ADC configurations for a hybrid multi-cloud environment with 2000 VPX instances, an administrator uses ADM 15.1 to orchestrate zero-trust access policies across AWS, Azure, and on-premises, automating config backups every 4 hours with retention of 30 days, encrypting backups with Kyber-1024 post-quantum algorithm, and integrating with HashiCorp Vault for key management. Which CLI command sequence configures the backup policy and encryption? (Select two)

A. add backup policy hybrid_backup -interval 4h -retention 30d -encryption KYBER-1024 -vaultIntegration HASICORP
B. create backup hybrid interval4 retain30 encrypt kyber vault hashi
C. set adm backup -policy hybrid_backup -pqAlgo KYBER-1024 -keyVault "vault.example.com" -schedule EVERY_4_HOURS -keep 30
D. configure backup policy 4h 30d kyber1024 vault hashi bind adm

Answer: A,C
Explanation: The add backup policy creates hybrid_backup with interval 4h for every 4 hours, retention 30d for 30 days, encryption KYBER-1024 for post-quantum security, vaultIntegration HASICORP for key management; the set adm backup applies pqAlgo KYBER-1024 equivalently, keyVault URL, schedule EVERY_4_HOURS, keep 30 for retention in ADM 15.1 hybrid orchestration.

Question: 736

An ADC Gateway must allow both SAML-based SSO and OAuth-based authentication for different services on the same vServer. What approach should you take? (Select one)

A. Use password authentication fallback
B. Bind respective authentication policies with expressions to match request context (URL, client type)
C. Set SAML and OAuth as secondary authentication
D. Choose only one protocol for the vServer

Answer: B
Explanation: ADC allows multiple authentication policies to be bound to a vServer and triggered by context-aware expressions, enabling protocol flexibility for different endpoints/services.

Question: 737

For regulatory audit readiness, how should Citrix ADC WAF logs be managed? (Select one)

A. Overwritten every 24 hours for storage savings

B. Disabled to improve latency
C. Forwarded to centralized SIEM with timestamping and integrity checks
D. Retained locally only until profile changes

Answer: C
Explanation: Evidence integrity and traceability are best preserved by forwarding logs (with tamper-evident stamps) to SIEM, supporting long-term auditability required for PCI-DSS.

Question: 738

You must configure a Citrix ADC HTTP Callout to GET data from a backend REST API, sending the original Host header and returning the total body length. Which CLI parameters are required? (Select all that apply)

A. -resultExpr
B. -urlStemExpr
C. -hostExpr
D. -httpMethod

Answer: A,B,C,D
Explanation: HTTP Callout configuration for a GET requires method and URL stem; hostExpr ensures original Host header is sent, while resultExpr extracts the required result, such as body length.

Question: 739

When enabling learning on a Web App Firewall profile, which must be true for secure production use? (Select one)

A. Only default WAF protections are enabled
B. All relaxations are applied automatically
C. Learning is disabled on all policies
D. Suggestions require explicit administrator approval

Answer: D
Explanation: To avoid introducing security gaps or false relaxations, all suggested relaxations must be reviewed and approved by an administrator before being enforced.

Question: 740

Tune HTTP in profiles for a API gateway: set -dropInvalidReq ENABLE**D.** What behavior in invalid

request scenarios? (Select one)

A. Logs and allows through
B. Forwards to error page
C. Rewrites invalid parts
D. Drops requests with malformed headers

Answer: D
Explanation: Enabling dropInvalidReq discards HTTP requests with invalid syntax or headers, enhancing security and performance by preventing processing of malformed traffic.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.