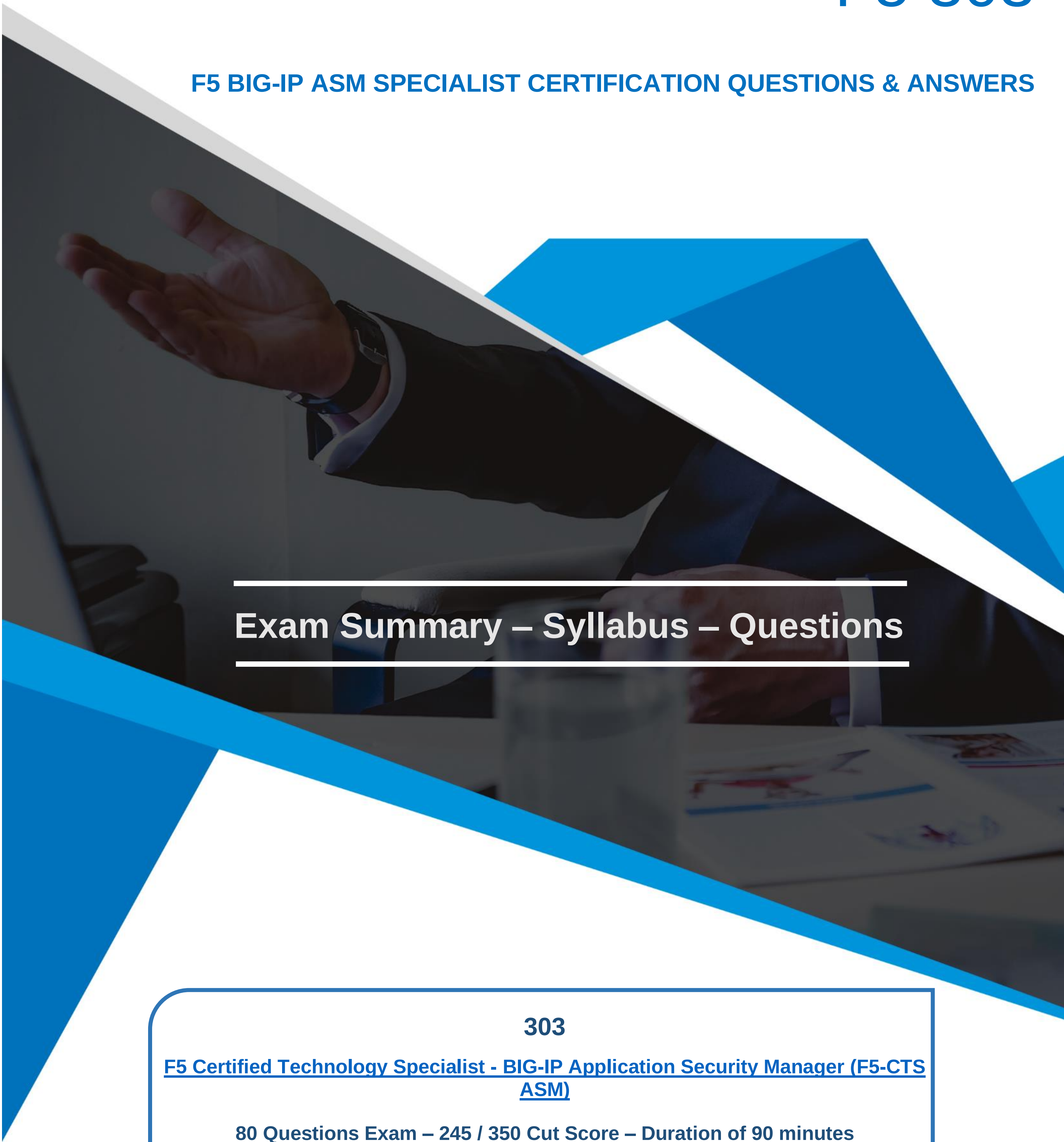
F5 303

F5 BIG-IP ASM SPECIALIST CERTIFICATION QUESTIONS & ANSWERS



Exam Summary – Syllabus – Questions

303

[F5 Certified Technology Specialist - BIG-IP Application Security Manager (F5-CTS ASM)](#)

80 Questions Exam – 245 / 350 Cut Score – Duration of 90 minutes

www.CertFun.com

Table of Contents

Know Your 303 Certification Well:

The 303 is best suitable for candidates who want to gain knowledge in the F5 Specialist. Before you start your 303 preparation you may struggle to get all the crucial BIG-IP ASM Specialist materials like 303 syllabus, sample questions, study guide.

But don't worry the 303 PDF is here to help you prepare in a stress free manner.

The PDF is a combination of all **your queries like**-

- What is in the 303 syllabus?
- How many questions are there in the 303 exam?
- Which Practice test would help me to pass the 303 exam at the first attempt?

Passing the 303 exam makes you F5 Certified Technology Specialist - BIG-IP Application Security Manager (F5-CTS ASM). Having the BIG-IP ASM Specialist certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

F5 303 BIG-IP ASM Specialist Certification Details:

Exam Name	F5 Certified Technology Specialist - BIG-IP Application Security Manager (F5-CTS ASM)
Exam Code	303
Exam Price	$180 (USD)
Duration	90 mins
Number of Questions	80
Passing Score	245 / 350
Books / Training	**F5 Training Programs**
Schedule Exam	**Pearson VUE**
Sample Questions	**F5 BIG-IP ASM Specialist Sample Questions**
Practice Exam	**F5 303 Certification Practice Exam**

303 Syllabus:

Topic	Details
ARCHITECTURE/DESIGN AND POLICY CREATION	
Explain the potential effects of common attacks on web applications	- Understand and describe how the ASM can affect clients and applications directly while in either transparent or blocking mode - Summarize the OWASP Top Ten
Explain how specific security policies mitigate various web application attacks	- Understand/interpret an iRule or LTM policy to map application traffic to an ASM policy - Explain the trade-offs between security, manageability, false positives, and performance
Determine the appropriate policy features and granularity for a given set of requirements	- Understand application (security) requirements and convert requirements to technical tasks
Determine which deployment method is most appropriate for a given set of requirements	- Determine which deployment method is most appropriate given the circumstances (web services, vulnerability scanner, templates, rapid deployment model)
Explain the automatic policy builder lifecycle	- Create any profiles required to support the policy deployment (xml, JSON, logging profiles) - Implement anomaly detection appropriate to the web app (D/Dos protection, brute force attack, web scraping, proactive bot defense)
Review and evaluate policy settings based on information gathered from ASM (attack signatures, DataGuard, entities)	- Configure initial policy building settings (automatic policy builder settings)
Define appropriate policy structure for policy elements	- Define appropriate policy structure for policy elements (URLs, parameters, file types, headers, sessions & logins, content profiles, CSRF protection, anomaly detection, DataGuard, proactive bot defense)

Topic	Details
Explain options and potential results within the deployment wizard	- Describe options within the deployment wizard (deployment method, attack signatures, virtual server, learning method - Select the appropriate ASM deployment model given the business requirements
Explain available logging options	- Explain the specifications of the remote logger (ports, types of logs, formats, address)
Describe the management of the attack signature lifecycle and select the appropriate attack signatures or signature sets	- Understand management of attack signature lifecycle (staging, enforcement readiness period) and select appropriate attack signatures or signature sets.
POLICY MAINTENANCE AND OPTIMIZATION	
Evaluate the implications of changes in the policy to the security and functionality of the application	- Evaluate whether the rules are being implemented effectively and appropriately to meet security and/or compliance requirements and make changes as appropriate
Explain the process to integrate natively supported third party vulnerability scan output and generic formats with ASM	- Refine appropriate policy structure for policy elements (URLs, parameters, file types, headers, sessions & logins, content profiles, CSRF protection, anomaly protection). - Explain how to manage policies using import, export, merge, and revert
Evaluate whether rules are being implemented effectively and appropriately to mitigate violations	- Evaluate the implications of changes in the policy to the security and vulnerabilities of the application
Determine how a policy should be adjusted based upon available data	- Tune an ASM policy for better performance, including use of wildcards to improve efficiency
Define the ASM policy management functions	- Identify the status of the policy - Define the violation types that exist in ASM - Describe how to merge and differentiate between policies

Topic	Details
REVIEW EVENT LOGS AND MITIGATE ATTACKS	
Interpret log entries and identify opportunities to refine the policy	- Examine traffic violations, determine if any attack traffic was permitted through the ASM and modify the policy to remove false positives - Locate and interpret reported security violations by end users and application developers
Given an ASM report, identify trends in support of security objectives.	- Understand and describe each major violation category and how ASM detects common exploits - Generate reporting for the ASM system and review the contents of the reports (anomaly statistics, charts, requests, PCI compliance status)
Determine the appropriate mitigation for a given attack or vulnerability	- Take appropriate action on reported security violations by end users and application developers - Modify ASM policy to adapt to attacks
Decide the appropriate method for determining the success of attack mitigation	- Choose an appropriate user defined attack signature to respond to particular traffic
TROUBLESHOOT	
Evaluate ASM policy performance issues and determine appropriate mitigation strategies	- Analyze performance graphs and statistics along with ASM configurations to determine the root cause of performance issues and appropriate remediation to the configuration based on guaranteed logging
Understand the impact of learning, alarm, and blocking settings on traffic enforcement	- Ensure that the security policy is inspecting web application traffic (application is functional and the policies are parsing the traffic)
Examine policy objects to determine why traffic is or is not generating violations	- Examine Security event logs and ASM configurations to determine expected violations based on the logging profile assigned to the virtual server
Identify and interpret ASM performance metrics	- Understand the impact of ASM iRules on performance. - Understand the impact of traffic spikes on ASM performance and available mitigation strategies

Topic	Details
Evaluate ASM system performance issues and determine appropriate mitigation strategies	- Correlate performance issues with ASM policy changes based on security policy history information and system performance graphs
Recognize ASM specific user roles and their permissions	- Recognize differences between user roles/permissions - Recognize ASM specific user roles

F5 303 Sample Questions:

Question: 1

What should an LTM Specialist configure on an LTM device to send AVR notification emails?

a) Custom SNMP traps on the LTM device for AVR notifications
b) Syslog on the LTM device to send to an SMTP server
c) Email notification to be sent via SMTP from the LTM device
d) Email notification to be sent via iControl from the LTM device

Answer: c

Question: 2

The network team introduces a new subnet 10.10.22.0/24 to the network. The route needs to be configured on the F5 device to access this network via the 30.30.30.158 gateway.

How should the LTM Specialist configure thisroute?

a) Tmsh changey net route 10.10.22/24 gw 30.30.30.158
b) Tmsh create net route 10.10.22/24 gw 30.30.30.158
c) Tmsh add net route 10.10.22/24 gw 30.30.30.158
d) Tmsh modify net route 10.10.22/24 gw 30.30.30.158

Answer: b

Question: 3

What should the 816-IP Administrator provide when opening a new ticket with F5 Support?

a) SSL private keys
b) Device root password
c) bigip.license file
d) QKViewfile

Answer: d

Question: 4

Remote office users are having performance issues with a virtual hosted on the F5 LTM. The LTM Specialist reviews the configuration for the virtual server and determine that some settings are set with default profiles.

Which profile should the LTM Specialist enable to improve virtual server performance?

a) An HTTP profile for the virtual server
b) A FastL4 profile on the virtual server
c) A WAN optimized client side profile
d) A Stream profile for the remote user networks

Answer: c

Question: 5

When importing a PEM formatted SSL certificate, which text needs to appear first in the file?

a) ...BEGIN CERTIFICATE....
b) --START CERTIFICATE....
c) ...SSL CERTIFICATE....
d) ...SECURITY CERTIFICATE....

Answer: a

Question: 6

Traffic to a pool of SFTP servers that share storage must be balanced by an LTM device. What are therequired profile and persistence settings for a standard virtual server?

a) tcp, ctientsst, ftp serverssl persistence
b) tcp - no persistence profile will be used
c) tcp, clientssl, serverssl persistence
d) tcp, ftp - Source address persistence

Answer: d

Question: 7

During a maintenance window, an EUD test was executed and the output displayed on the screen. The BIG-IP Administrator did NOT save the screen output. The BIG-IP device is currently handling business critical traffic. The BIG-IP Administrator needs to minimize impact. What should the BIG-IP Administrator do to provide the EUD results to F5 Support?

a) Execute EUD from tmsh and collect output from console
b) Collect file /var/log/messages
c) Collect file /shared/log/eud.log
d) Boot the device into EUD then collect output from console

Answer: c

Question: 8

Which file should be modified to create custom SNMP alerts?

a) /config/user_alert.conf
b) /etc/alertd/user_alert.conf
c) /etc/alertd/alert.conf
d) /config/alert.conf

Answer: a

Question: 9

Which file should the BIG-IP Administrator check to determine when a Virtual Server changed its status?

a) /var/log/audit
b) /var/log/lastlog
c) /var/log/monitors
d) /var/log/tm

Answer: d

Question: 10

A BIG-IP Administrator is creating a new Trunk on the BIG-IP device. What objects should be added to the new Trunk being created?

a) Interfaces
b) Network routes
c) VLANS
d) IP addresses

Answer: a

Study Guide to Crack F5 BIG-IP ASM Specialist 303 Exam:

- Getting details of the 303 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the 303 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the F5 provided training for 303 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.

- Read from the 303 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on 303 practice tests is must. Continuous practice will make you an expert in all syllabus areas.