EXAM BLUEPRINT

# 303 — BIG-IP ASM Specialist

## ABOUT THE *303 – BIG-IP ASM SPECIALIST* EXAM

The *303 – BIG-IP ASM Specialist* exam identifies individuals who are qualified to design, implement, and maintain ASM, including advanced features. They will likely be a senior network, system, and/or application security engineer with at least one year of relevant job experience responsible for delivering highly available, scalable, and secure applications with the ASM technology. The BIG-IP ASM Specialist understands the underlying principles of ASM and can draw on that insight to integrate ASM with other platforms and products.

## WHAT IS THE *303 – BIG-IP ASM SPECIALIST* EXAM BLUEPRINT?

F5 Certified exam blueprints list all the objectives an exam has to measure, much like a syllabus for the exam itself. Blueprints provide a detailed breakdown of the skills and knowledge a candidate should have to pass the exam. They contain section levels, objectives and examples, and can be used to identify areas for additional study. The examples are illustrative, not exhaustive.

F5 Certification exams are designed to test the knowledge, skills, and abilities of the candidate. These exams are not designed to test version-specific TMOS features, but rather assess knowledge and understanding of F5 technology solutions for which the exam is developed. Refer to individual exam blueprints for exam publication date.

## PREREQUISITE:

F5 Certified BIG-IP Administrator (F5-CA)

## CREDENTIAL AWARDED:

F5 Certified Technology Specialist, BIG-IP ASM

# 303 – BIG-IP ASM Specialist

| Section 1 : ARCHITECTURE/DESIGN AND POLICY CREATION | | |
|---|---|---|
| **Objectives and Examples** | | **CC*** |
| **1.01** | **Explain the potential effects of common attacks on web applications**<br>• Understand and describe how the ASM can affect clients and applications directly while in either transparent or blocking mode<br>• Summarize the OWASP Top Ten | **U/A** |
| **1.02** | **Explain how specific security policies mitigate various web application attacks**<br>• Understand/interpret an iRule or LTM policy to map application traffic to an ASM policy<br>• Explain the trade-offs between security, manageability, false positives, and performance | **U/A** |
| **1.03** | **Determine the appropriate policy features and granularity for a given set of requirements**<br>• Understand application (security) requirements and convert requirements to technical tasks | **A/E** |
| **1.04** | **Determine which deployment method is most appropriate for a given set of requirements**<br>• Determine which deployment method is most appropriate given the circumstances (web services, vulnerability scanner, templates, rapid deployment model) | **A/E** |
| **1.05** | **Explain the automatic policy builder lifecycle**<br>• Create any profiles required to support the policy deployment (xml, JSON, logging profiles)<br>• Implement anomaly detection appropriate to the web app (D/DoS protection, brute force attack, web scraping, proactive bot defense) | **U/A** |
| **1.06** | **Review and evaluate policy settings based on information gathered from ASM (attack signatures, DataGuard, entities)**<br>• Configure initial policy building settings (automatic policy builder settings) | **A/E** |
| **1.07** | **Define appropriate policy structure for policy elements**<br>• Define appropriate policy structure for policy elements (URLs, parameters, file types, headers, sessions and logins, content profiles, CSRF protection, anomaly detection, DataGuard, proactive bot defense) | **U/A** |
| **1.08** | **Explain options and potential results within the deployment wizard**<br>• Describe options within the deployment wizard (deployment method, attack signatures, virtual server, learning method<br>• Select the appropriate ASM deployment model given the business requirements | **U/A** |
| **1.09** | **Explain available logging options**<br>• Explain the specifications of the remote logger (ports, types of logs, formats, address) | **R** |
| **1.10** | **Describe the management of the attack signature lifecycle and select the appropriate attack signatures or signature sets**<br>• Understand management of attack signature lifecycle (staging, enforcement readiness period) and select appropriate attack signatures or signature sets. | **U/A** |

* Cognitive Complexity Key: **R** = Remember, **A/E** = Analyze/Evaluate, **U/A** = Understand/Apply

| Section 2 : POLICY MAINTENANCE AND OPTIMIZATION | | |
|---|---|---|
| **Objectives and Examples** | | **CC*** |
| **2.01** | **Evaluate the implications of changes in the policy to the security and functionality of the application**<br>• Evaluate whether the rules are being implemented effectively and appropriately to meet security and/or compliance requirements and make changes as appropriate | **A/E** |
| **2.02** | **Explain the process to integrate natively supported third party vulnerability scan output and generic formats with ASM**<br>• Refine appropriate policy structure for policy elements (URLs, parameters, file types, headers, sessions and logins, content profiles, CSRF protection, anomaly protection)<br>• Explain how to manage policies using import, export, merge, and revert | **U/A** |
| **2.03** | **Evaluate whether rules are being implemented effectively and appropriately to mitigate violations**<br>• Evaluate the implications of changes in the policy to the security and vulnerabilities of the application | **A/E** |
| **2.04** | **Determine how a policy should be adjusted based upon available data**<br>• Tune an ASM policy for better performance, including use of wildcards to improve efficiency | **A/E** |
| **2.05** | **Define the ASM policy management functions**<br>• Identify the status of the policy<br>• Define the violation types that exist in ASM<br>• Describe how to merge and differentiate between policies | **R** |

| Section 3 : REVIEW EVENT LOGS AND MITIGATE ATTACKS | | |
|---|---|---|
| **Objectives and Examples** | | **CC*** |
| **3.01** | **Interpret log entries and identify opportunities to refine the policy**<br>• Examine traffic violations, determine if any attack traffic was permitted through the ASM and modify the policy to remove false positives<br>• Locate and interpret reported security violations by end users and application developers | **A/E** |
| **3.02** | **Given an ASM report, identify trends in support of security objectives**<br>• Understand and describe each major violation category and how ASM detects common exploits<br>• Generate reporting for the ASM system and review the contents of the reports (anomaly statistics, charts, requests, PCI compliance status) | **U/A** |
| **3.03** | **Determine the appropriate mitigation for a given attack or vulnerability**<br>• Take appropriate action on reported security violations by end users and application developers<br>• Modify ASM policy to adapt to attacks | **A/E** |

* Cognitive Complexity Key: **R** = Remember, **A/E** = Analyze/Evaluate, **U/A** = Understand/Apply

| | | |
|---|---|---|
| **3.04** | **Decide the appropriate method for determining the success of attack mitigation**<br>• Choose an appropriate user defined attack signature to respond to particular traffic | **A/E** |

| Section 4 : TROUBLESHOOT | | |
|---|---|---|
| **Objectives and Examples** | | **CC*** |
| **4.01** | **Evaluate ASM policy performance issues and determine appropriate mitigation strategies**<br>• 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 | **A/E** |
| **4.02** | **Understand the impact of learning, alarm, and blocking settings on traffic enforcement**<br>• Ensure that the security policy is inspecting web application traffic (application is functional and the policies are parsing the traffic) | **U/A** |
| **4.03** | **Examine policy objects to determine why traffic is or is not generating violations**<br>• Examine Security Event Logs and ASM configurations to determine expected violations based on the logging profile assigned to the virtual server | **A/E** |
| **4.04** | **Identify and interpret ASM performance metrics**<br>• Understand the impact of ASM iRules on performance.<br>• Understand the impact of traffic spikes on ASM performance and available mitigation strategies | **U/A** |
| **4.05** | **Evaluate ASM system performance issues and determine appropriate mitigation strategies**<br>• Correlate performance issues with ASM policy changes based on security policy history information and system performance graphs | **A/E** |
| **4.06** | **Recognize ASM specific user roles and their permissions**<br>• Recognize differences between user roles/permissions<br>• Recognize ASM specific user roles | **R** |

* Cognitive Complexity Key: **R** = Remember, **A/E** = Analyze/Evaluate, **U/A** = Understand/Apply

# Exam Details

### HOW MUCH DO F5 EXAMS COST?

All F5 exams are currently priced at US$180 (not including local taxes and fees) per exam, per attempt.

### HOW LONG ARE F5 EXAMS?

This exam is 90 minutes long (not including any non-native English or other accommodations).

### WHAT IS THE PASSING SCORE FOR F5 EXAMS?

F5 exams require a passing score of 245 out of a range between 100 and 350.

### SCALED SCORING

Scaled scores ensure that the reported scores across exam forms and versions have the same meaning regardless of difficulty. Fair and consistent decisions can then be made about exam results regardless of the exam form or version. More information ›

### HOW MANY QUESTIONS ARE THERE?

This exam has 80 questions (70 items that are scored, 10 pilot/beta items).

### WHAT FORMAT ARE F5 EXAMS?

F5 exams are all computer-based, multiple-choice-response exams. Some questions contain exhibits or scenarios that you will need to view in order to answer the question.

### WHAT IS THE F5 RETAKE POLICY?

**1st failure:** Exam hold for 15 days (You cannot take the exam again for 15 days.)
**2nd failure:** Exam hold for 30 days
**3rd failure:** Exam hold for 45 days
**4th failure:** Exam hold for 365 days
**5th and subsequent failed attempts:** 90 days

# Cognitive Complexity Descriptions

Lower Order Thinking Skills → Higher Order Thinking Skills

| Remember | Understand/Apply | Analyze/Evaluate | Create |
|---|---|---|---|
| Information retrieval | Knowledge transfer | Critical thinking and reasoning | Innovation or creative thinking |
| Rote memorization | Comprehension or ability to apply knowledge to a standard process | Determine how parts relate to whole or knowledge integration and application to new situations | Forming an original work product |
| Retrieve relevant knowledge from long-term memory | Construct meaning from information | Make judgments based on criteria | Combine or reorganize parts to form a new pattern or structure |
| E.g., recall, retrieve, recognize | E.g., interpret, classify, compare, explain, implement | E.g., troubleshoot, attribute, diagnose, critique | E.g., generate, plan, produce |

Alpine Testing Solutions' suggested cognitive complexity levels and associated verb references consider multiple approaches to defining cognitive processing (e.g., Anderson et al., Webb, Bloom, Frisbie). Above material created with assistance from Alpine and distributed with Alpine's permission as an attachment to certification test

Alpine

Alpine Testing Solutions, Inc. (Alpine) gives F5 Networks permission to distribute the PDF "Cognitive Complexity Description 20130418.pdf" as an attachment to certification test blueprints created with assistance from Alpine into the exam blueprint.