304 - APM TECHNOLOGY SPECIALIST
EXAM BLUEPRINT

ABOUT THE 304-APM TECHNOLOGY SPECIALIST EXAM.
The 304-APM Technology Specialist exam is the required to achieve Certified F5 Technology Specialist, APM status.

Successful completion of the APM Technology Specialist exam acknowledges the skills and understanding necessary for day-to-day management of Application Delivery Networks (ADNs) that incorporate technologies based on the F5 TMOS operating system (v11).

WHAT IS THE 304-APM TECHNOLOGY SPECIALIST EXAM BLUEPRINT?
F5 Certified Exam Blueprints list all the objectives an exam has to measure, much like a syllabus for the exam itself. The blueprint provides the detailed breakdown of the skills and knowledge a candidate should have to pass the exam. Blueprints can be used to identify areas for additional study, and are best used in conjunction with the Exam Study Guides.

PREREQUISITE:
F5 Certified BIG-IP Administrator (F5-CA)

CREDENTIAL AWARDED:
F5 Certified Technology Specialist, APM

THIS EXAM IS BASED ON V11.3

304 - APM TECHNOLOGY SPECIALIST

EXAM BLUEPRINT

Section 1:	Assess security needs and requirements to create an APM policy	Cognitive Complexity
Objective 1.01	Explain how APM mitigates common attack vectors and methodologies (e.g., cookie hijacking [front and back], DoS attack)	U/A
Objective 1.02	Identify which APM tool(s) should be used to mitigate a specific authentication attack	R
Examples	Describe common attack vectors Describe cookie function in common browsers Compare authentication methods	
Objective 1.03	Explain how APM uses and manages session cookies (domain, host, multi-domain)	U/A
Examples	Determine endpoint inspection requirements (e.g., OPSWAT, registry check). Describe the process to mitigate password guessing attacks	
Objective 1.04	Explain the differences among access methods (e.g., network, portal, access management)	U/A
Objective 1.05	Determine the appropriate access method for a use case or set of requirements	U/A
Examples	Distinguish among network communication requirements, security requirements, reporting requirements, and note the pros and cons Explain how security permissions on client PCs affect use cases	
Objective 1.06	Explain how APM interacts with commonly used applications (e.g., Microsoft Exchange, Citrix, VMware View, SharePoint)	U/A
Examples	Explain how APM interacts with a virtual desktop infrastructure (e.g., VMware View, Citrix, RDP) Compare access modes Determine deployment configurations with commonly used applications	
Objective 1.07	Explain the differences among logging levels (e.g., performance implications, security implications, information provided)	U/A
Examples	Explain how APM uses TMOS facilities for logging Interpret log messages and the data contained within them	
Objective 1.08	Determine appropriate logging methods and verbosity levels to meet specified requirements	U/A
Examples	Explain the various levels of verbosity available Determine appropriate verbosity levels Explain the performance implications of extended logging Explain security and privacy implications of log settings	

Cognitive Complexity Key:
R=Remember
U/A=Understand/Evaluate
C=Create

Section 2:	Configure and deploy an access profile	Cognitive Complexity
Objective 2.01	Determine the circumstances under which it is appropriate to use an APM specific profile (i.e., access, connectivity, rewrite, VDI and Java support)	U/A
Examples	Determine appropriate access policy configurations to assign to the virtual server Given access methods, determine profiles and options that should be configured	
Objective 2.02	Determine the circumstances under which it is appropriate to use a non-APM specific profile (e.g., ServerSSL, Web Acceleration, Compression)	U/A
Examples	Determine the circumstances under which particular access policy profiles and options are appropriate Compare non-APM Specific profiles when configuring a virtual server	
Objective 2.03	Explain how to create and assign an SSL profile	U/A
Examples	Describe the process to upload the SSL certificate and key Determine which SSL profile to assign to the virtual server	
Objective 2.04	Determine appropriate SNAT settings to meet access requirements for Network Access (e.g., VoIP, Active mode FTP, Remote Desktop to Network Access Clients)	U/A
Examples	When troubleshooting failing connections, determine appropriate SNAT settings based on access requirements Compare SNAT pool options	
Objective 2.05	Explain the characteristics (e.g., pros and cons, restrictions, security implications, HA setup) of available AAA profiles	U/A
Examples	Distinguish among/compare and contrast the different AAA types	
Objective 2.06	Explain the characteristics (e.g., pros and cons, restrictions, security implications) of available SSO profiles	U/A
Examples	Distinguish among/compare and contrast the different SSO types	
Objective 2.07	Explain the implications of passwordless authentication options in APM and how they affect SSO (e.g., SAML, Client certificate, NTLM-end-user)	U/A
Examples	Explain how APM uses TMOS facilities for logging Interpret log messages and the data contained within them	
Objective 2.08	Explain how to configure AAA profiles (e.g., HTTP Basic, AD, LDAP, Radius, TACACS, KERBEROS, RSA, SAML, OCSP, CRLDP)	U/A

Cognitive Complexity Key:
R=Remember
U/A=Understand/Apply
C=Create

Objective 2.09	Explain techniques to simultaneously configure multiple AAA profiles (e.g., two-factor)	U/A
Examples	Explain high availability options for AAA profiles Describe the differences and similarities between authentication methods Explain the process to set up an APM device to use HTTPS Authentication	
Objective 2.10	Explain how to configure SSO profiles (e.g., HTTP Basic, NTLM, KERBEROS, SAML, Forms)	U/A
Examples	Describe SSO profiles Determine the correct configurations to resolve SSO performance issues	
Objective 2.11	Explain how to configure SAML use cases (e.g., IDP, SP, IDP-initiated, SP-initiated)	U/A
Examples	Configure SAML federation between two BIG-IPs	
Objective 2.12	Describe how to add and remove client and machine certificates	R
Objective 2.13	Determine appropriate deployment option(s) to meet network access requirements (e.g., standalone edge client, browser components, mobile apps)	R
Examples	Describe the different access methods: portal access functionality, app tunnel functionality, network access functionality, LTM+APM functionality List APM device clients When deploying a Network Access Edge client solution, determine which Edge Client component is required	
Objective 2.14	Explain how to configure access methods (e.g., network [SNAT vs. Routed Mode], portal [rewrite options], application, app tunnel, LTM+APM)	U/A
Examples	Determine best deployment option for network access (e.g., standalone edge client, browser components, mobile apps) Configure application access (e.g., app tunnel, RDP, VDI) Explain protocol restrictions on application tunnels (i.e., TCP) Determine when Java support is needed for RDP (e.g., Mac and Linux clients) Configure portal access Explain the custom rewrite options (e.g., split tunnel, client caching)	
Objective 2.15	Determine appropriate access methods (e.g., network, portal, application, LTM+APM) to meet requirements	U/A
Objective 2.16	Explain how to configure and assign ACLs (e.g., L4, L7, static, dynamic, default action, iRule events, logging options)	U/A

Cognitive Complexity Key:
R=Remember
U/A=Understand/Apply
C=Create

Examples	Explain the difference between Layer 7 and Layer 4 ACLs Explain the difference between static and dynamic Explain how ACLs are processed Explain the default ACL action (e.g., default allow) Describe ACL logging options	
Objective 2.17	Identify resource types for which associated ACLs are automatically created (e.g., remote desktop, portal access, application tunnels)	R
Objective 2.18	Describe the ACL action types and their functions (e.g., allow, continue, discard, reject)	R
Examples	Identify the ACL action types (e.g., allow, continue, discard, reject)	
Objective 2.19	Describe methods to map Microsoft Active Directory groups to assigned resources	R
Objective 2.20	Explain the use of APM session variables (e.g., session flow, use in iRules, variable assign policy item)	U/A
Examples	Determine which Use the iRule event policy item in the VPE Determine the appropriate Access Policy modifications to meet specific authentication requirements	
Objective 2.21	Explain access policy flow and logic (i.e., branching, loops, macros [when and how to use them])	U/A
Objective 2.22	Describe the use and configuration of endpoint checks (e.g., registry check, process check, Windows info, machine cert auth)	U/A
Examples	Configure endpoint checks: AV check, registry check, file check, firewall check, process check, machine certification check Determine which steps are necessary to add macro checks to a policy Determine which steps are necessary to take when adding authentication methods	
Objective 2.23	Describe customization options for an access policy (logon page, webtop, network access, language)	R
Examples	Describe the different endpoint checks Identify the policy items available (e.g., client side, service side, general purpose) Describe the different branch endings (e.g., allow, deny, redirect)	
Section 3:	**Maintain APM access profiles**	Cognitive Complexity
Objective 3.01	Interpret device performance information (e.g., dashboard, statistics tab, ACL denied report)	U/A

Cognitive Complexity Key:
R=Remember
U/A=Understand/Apply
C=Create

Objective 3.02	Identify necessary software maintenance procedures to address a given condition	R
Examples	List the steps for a safe upgrade (e.g., perform a backup before upgrading) Describe an OPSWAT integration Determine the most appropriate monitoring facility within the BIG-IP WebUI Predict the behavior of a device when upgrading and/or adding a new device Describe what happens during an upgrade if an active APM device was to failover to standby	
Objective 3.03	Determine how upgrades on production systems affect end users (e.g., client components and high availability failover)	U/A
Section 4:	**Identify and resolve APM issues**	Cognitive Complexity
Objective 4.01	Explain the purpose and function of client side components (e.g., DNS Proxy Relay service, Component Installer service for Windows, User Logon Credentials Access Service for Windows)	U/A
Objective 4.02	Interpret client and machine certificates (e.g., subject, issuer)	U/A
Examples	Describe the process when configuring client certificates Give examples of Access resource types	
Objective 4.03	Interpret an HTTP protocol trace collected with a client side tool (e.g., HTTPWatch, Fiddler, Paros, Live Headers)	U/A
Examples	Perform and interpret HTTPWatch capture Describe SSO methods for an APM-delivered web application	
Objective 4.04	Explain how to use capture utilities (e.g., SSLDump and TCPDump)	U/A
Examples	Perform and interpret output of TCPDump Determine the correct TCPDump and SSLDump to resolve specific issues	
Objective 4.05	Analyze and interpret APM-specific log files (e.g., APM, SSO, rewrite)	U/A
Examples	Identify error messages in log file outputs Determine the root cause of login issues based on information provided in log files	
Objective 4.06	Describe the use of built-in trouble-shooting tools (e.g., web engine trace, F5 Troubleshooting Utility, SessionDump, ADTest tool, LDAP search)	R
Examples	Locate error codes List and describe APM logging services Locate core files	

Cognitive Complexity Key:
R=Remember
U/A=Understand/Apply
C=Create

Objective 4.07	Diagnose and resolve authentication issues (e.g., client>APM, APM>AAA, APM>SSO)	A/E
Examples	Analyze http requests to determine authentication issues	
Objective 4.08	Diagnose and resolve client side issues related to connections, performance, and endpoint inspection	A/E
Examples	Determine the root cause of authentication and client side issues Differentiate between different types of authentication and client side issues	

Cognitive Complexity Key:
R=Remember
U/A=Understand/Apply
C=Create

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 situation(s)	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 blueprints.

Alpine Testing Solutions

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.