Purpose of this Document

The 304-APM Specialist exam is the second exam required to achieve F5 Certified Technology Specialist, Access Policy Manager (F5-CTS, APM) status.

This document outlines topic areas covered on the F5 APM Specialists Certification Exam and resources available to help prepare test takers.

References

F5 Training: Configuring BIG-IP APM v11 Access Policy Manager, October 2013, V11.4.0 Edition (Configuring BIG-IP APM, Chapter XX)

Section 1: Assess security needs and requirements to create an APM policy

Objective 1.01: Explain how APM mitigates common attack vectors and methodologies (e.g., cookie hijacking [front and back], DoS attack)

- SOL12300 - Overview of access policy timeout settings
- Understanding access profile settings 11.4.0 Configuration Guide for BIG-IP APM, Ch5

Objective 1.02: Identify which APM tool(s) should be used to mitigate a specific authentication attack

Describe common attack vectors

- SOL14813 - Detecting and mitigating DoS/DDoS attacks (11.4.x - 11.5.x)
- SOL10260 - Mitigating Slowloris denial-of-service (DoS) attacks with the BIG-IP system

Describe cookie function in common browsers

Compare authentication methods

- SOL11446 - Configuring HTTP authentication options for BIG-IP APM
- SOL13027 - Configuring HTTP basic authentication for the BIG-IP APM system
- SOL12964 - Configuring HTTP form-based authentication using URL matching for BIG-IP APM
- SOL12966 - Configuring HTTP form authentication using string matching for the BIG-IP APM
- SOL12965 - Configuring HTTP form-based authentication using cookie matching for the BIG-IP APM system
**Objective 1.03: Explain how APM uses and manages session cookies (domain, host, multi-domain)**

Determine endpoint inspection requirements (e.g., OPSWAT, registry check).

- SOL12385 - OPSWAT support chart
- SOL14207 - Determining the active OPSWAT version
- SOL10942 - Installing OPSWAT hotfixes on BIG-IP APM systems
- SOL14947 - The BIG-IP Edge Client components for Mac OS X
- SOL14045 - The BIG-IP Edge Client components for Windows
- SOL12444 - Overview of the Component Troubleshooting Utility

Describe the process to mitigate password guessing attacks

**Objective 1.04: Explain the differences among access methods (e.g., network, portal, access management)**

- Understanding BIG-IP Access Policy Manager access types 11.4.0 Configuration Guide for BIG-IP APM Ch1
- Configuring BIG-IP APM, Chapters 4, 5 and 7

**Objective 1.05: Determine the appropriate access method for a use case or set of requirements**

Distinguish among network communication requirements, security requirements, reporting requirements, and note the pros and cons

- SOL12227 - Configuring the BIG-IP APM portal access for the F5 BIG-IP Edge Portal application
- SOL12644 - Overview of the BIG-IP Edge Portal application for Android devices
- Understanding available actions 11.4.0 Configuration Guide for BIG-IP APM Ch4

Explain how security permissions on client PCs affect use cases

- Configuring BIG-IP APM, Chapters 4, 5 and 7

**Objective 1.06: Explain how APM interacts with commonly used applications (e.g., Microsoft Exchange, Citrix, VMware View, SharePoint)**

Explain how APM interacts with a virtual desktop infrastructure (e.g., VMware View, Citrix, RDP)

- SOL13738 - iApp: Citrix XenApp / XenDesktop
- SOL15041 - iApp: VMware View and Horizon View

Compare access modes

- Understanding BIG-IP Access Policy Manager access types 11.4.0 Configuration Guide for BIG-IP APM Ch1
Determine deployment configurations with commonly used applications

- SOL13201 -Deploying F5 with VMware View 5.0 and 5.1
- SOL11166 - Deploying F5 with VMware Virtual Desktop Infrastructure (VDI)
- BIG-IP Access Policy Manager: VMware Horizon View Integration Implementations
- BIG-IP Access Policy Manager: Hosted Content Implementations

**Objective 1.07: Explain the differences among logging levels (e.g., performance implications, security implications, information provided)**

Explain how APM uses TMOS facilities for logging

- SOL11253 - Session variable logging within an access policy
- SOL13394 - Overview of BIG-IP APM logging destinations
- SOL11124 - Configuring the BIG-IP APM system to log session variables
- SOL13595 - Frequently used tools for troubleshooting BIG-IP APM and Edge Gateway issues (11.x)

Interpret log messages and the data contained within them

- [Logging and Reporting](#) 11.4.0 Configuring Guide for BIG-IP APM, Ch12

**Objective 1.08: Determine appropriate logging methods and verbosity levels to meet specified requirements**

- 11.4.0 Configuration Guide for BIG-IP Access Policy Manager, Chapter 12

Explain the various levels of verbosity available

Determine appropriate verbosity levels

- SOL13317 - Configuring the level of information that syslog-ng sends to log files (11.x)

Explain the performance implications of extended logging

- SOL14303 - A BIG-IP APM system that processes a high volume of traffic may experience excessively large BIG-IP APM log files

Explain security and privacy implications of log settings

- SOL13080 - Configuring the BIG-IP system to log to a remote syslog server (11.x)

**Section 2: Configure and deploy an access profile**

**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)**

Determine appropriate access policy configurations to assign to the virtual server

© 2013 F5 Networks, Inc.
• Understanding BIG-IP Access Policy Manager access types  11.4.0 Configuration Guide for BIG-IP APM Ch1
• What is network access?  11.4.0 APM NA Configuration Guide
• Overview: What is portal access?  11.4.0 APM PA Configuration Guide
• What are app tunnels?  11.4.0 APM App Access Guide

Given access methods, determine profiles and options that should be configured

• Configuring Network Access Resources  11.4.0 APM NA Configuration Guide
• Configuring Resources for Portal Access  11.4.0 APM PA Configuration Guide
• Configuring Remote Desktop Access  11.4.0 APM App Access Guide
• Configuring Webtops  11.4.0 APM App Access Guide

• Configuring BIG-IP APM, Chapter 7

Objective 2.02: Determine the circumstances under which it is appropriate to use a non-APM specific profile (e.g., ServerSSL, Web Acceleration, Compression)

Determine the circumstances under which particular access policy profiles and options are appropriate

• Configuration Guide for BIG-IP Access Policy Manager
• BIG-IP Access Policy Manager Customization Guide

Compare non-APM Specific profiles when configuring a virtual server

• SOL14903 - Overview of the Web Acceleration profile
• Compressing HTTP Responses  11.4.0 BIG-IP Local Traffic Manager: Implementations
• SOL8802 - Using SSL ciphers with BIG-IP Client SSL and Server SSL profiles

Objective 2.03: Explain how to create and assign an SSL profile

• SOL14783 - Overview of the Client SSL profile (11.x)
• SOL14806 - Overview of the Server SSL profile (11.x)

Describe the process to upload the SSL certificate and key

• SOL14620 - Managing SSL certificates for BIG-IP systems

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)
When troubleshooting failing connections, determine appropriate SNAT settings based on access requirements

Compare SNAT pool options

- SOL7820 - Overview of SNAT features
- SOL13782 - The BIG-IP APM network access tunnel does not use a floating IP address
- Selecting a route domain or SNAT 11.4.0 Configuration Guide for BIG-IP APM Ch6
- Configuring BIG-IP APM, Chapters 5 and 8

Objective 2.05: Explain the characteristics (e.g., pros and cons, restrictions, security implications, HA setup) of available AAA profiles

Distinguish among/compare and contrast the different AAA types

- Authentication Concepts 11.4.0 BIG-IP APM Authentication Configuration Guide
- SOL11446 - Configuring HTTP authentication options for BIG-IP APM
- SOL14720 - Configuring user authentication for single-user mode access
- SOL14287 - Route domain support for BIG-IP APM Active Directory AAA servers
- SOL14997 - The BIG-IP APM RADIUS AAA configuration profiles support only the PAP encryption method

Objective 2.06: Explain the characteristics (e.g., pros and cons, restrictions, security implications) of available SSO profiles

Distinguish among/compare and contrast the different SSO types

- Single Sign-On Methods 11.4.0 BIG-IP APM: Single Sign-On Configuration
- Understanding Single-Sign On settings 11.4.0 Configuration Guide for BIG-IP APM Ch5
- Configuring BIG-IP APM, Chapters 4, 7, 13 and 14

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)

- SOL12169 - Configuring passwordless client certificate authentication

Explain how APM uses TMOS facilities for logging

- SOL13394 - Overview of BIG-IP APM logging destinations

Interpret log messages and the data contained within them

- Understanding log content 11.4.0 Configuration Guide for BIG-IP APM Ch12
- SOL13595 - Frequently used tools for troubleshooting BIG-IP APM and Edge Gateway issues (11.x)
- SOL14184 - Troubleshooting BIG-IP APM portal applications
- SOL13384: Performing a web applications trace (11.x)
Objective 2.08: Explain how to configure AAA profiles (e.g., HTTP Basic, AD, LDAP, Radius, TACACS, KERBEROS, RSA, SAML, OCSP, CRLDP)

- BIG-IP Access Policy Manager Authentication Configuration Guide
- Configuring BIG-IP APM, Chapters 2 and 10

Objective 2.09: Explain techniques to simultaneously configure multiple AAA profiles (e.g., two-factor)

Explain high availability options for AAA profiles

- AAA and Configuring High Availability 11.4.0 BIG-IP APM Authentication Configuration Guide

Describe the differences and similarities between authentication methods

- Authentication Concepts 11.4.0 BIG-IP APM Authentication Configuration Guide

Explain the process to set up an APM device to use HTTPS Authentication

- Task summary for configuring HTTPS authentication 11.4.0 BIG-IP APM Authentication Configuration Guide
- Configuring BIG-IP APM, Chapters 10 and 12

Objective 2.10: Explain how to configure SSO profiles (e.g., HTTP Basic, NTLM, KERBEROS, SAML, Forms)

Describe SSO profiles

- SOL11312 - Creating network access with single-sign on capabilities
- SOL13510 - Overview of the Kerberos SSO GSSAPI header
- SOL11312 - Creating network access with single-sign on capabilities
- SOL13751 - Using session variables in Single Sign-On objects

Determine the correct configurations to resolve SSO performance issues

- Configuring BIG-IP APM, Chapter 4, 7, 13 and 14

Objective 2.11: Explain how to configure SAML use cases (e.g., IDP, SP, IDP-initiated, SP-initiated)

- BIG-IP Access Policy Manager: SAML Configuration

Configure SAML federation between two BIG-IPs

- BIG-IP System Federation for SP-Initiated Connections 11.4.0 BIG-IP APM SAML Configuration
- BIG-IP System Federation for SP- and IdP-Initiated Connections 11.4.0 BIG-IP APM SAML Configuration

Objective 2.12: Describe how to add and remove client and machine certificates

- SOL14620 - Managing SSL certificates for BIG-IP systems
Objective 2.13: Determine appropriate deployment option(s) to meet network access requirements (e.g., standalone edge client, browser components, mobile apps)

Describe the different access methods: portal access functionality, app tunnel functionality, network access functionality, LTM+APM functionality

- SOL12488 - BIG-IP Edge Client and BIG-IP Edge Portal comparison
- SOL12328 - Overview of the iOS BIG-IP Edge Portal application for Apple iPhone, iPad, and iPod touch

List APM device clients

- BIG-IP APM Client Compatibility Matrix

When deploying a Network Access Edge client solution, determine which Edge Client component is required

- SOL14045 - The BIG-IP Edge Client components for Windows
- SOL14947 - The BIG-IP Edge Client components for Mac OS X
- Configuring BIG-IP APM, Chapter 5

Objective 2.14: Explain how to configure access methods (e.g., network [SNAT vs. Routed Mode], portal [rewrite options], application, app tunnel, LTM+APM)

Determine best deployment option for network access (e.g., standalone edge client, browser components, mobile apps)

- BIG-IP Access Policy Manager: Network Access Configuration

Configure application access (e.g., app tunnel, RDP, VDI)


Explain protocol restrictions on application tunnels (i.e., TCP)

- Configuring App Tunnel Access 11.4.0 APM App Access Guide

Determine when Java support is needed for RDP (e.g., Mac and Linux clients)

- Configuring Remote Desktop Access 11.4.0 APM App Access Guide

Configure portal access

- BIG-IP Access Policy Manager: Portal Access

Explain the custom rewrite options (e.g., split tunnel, client caching)

- Configuring Rewrite Profiles for Portal Access 11.4.0 APM PA Guide
- Configuring BIG-IP APM, Chapters 4, 5 and 7

Objective 2.15: Determine appropriate access methods (e.g., network, portal, application, LTM+APM) to meet requirements

- Configuring BIG-IP APM, Chapter 4, 5 and 7

© 2013 F5 Networks, Inc.
Objective 2.16: Explain how to configure and assign ACLs (e.g., L4, L7, static, dynamic, default action, iRule events, logging options)
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
- Configuring BIG-IP APM, Chapter 6
  SOL14998 - BIG-IP APM access policy ACLs and network access tunnels

Objective 2.17: Identify resource types for which associated ACLs are automatically created (e.g., remote desktop, portal access, application tunnels)
- Configuring BIG-IP APM, Chapter 6
  SOL13425 - Overview of APM Web Applications
  SOL12644 - Overview of the BIG-IP Edge Portal application for Android devices
  SOL12328 - Overview of the iOS BIG-IP Edge Portal application for Apple iPhone, iPad, and iPod touch

Objective 2.18: Describe the ACL action types and their functions (e.g., allow, continue, discard, reject)
Identify the ACL action types (e.g., allow, continue, discard, reject)
- Configuring BIG-IP APM, Chapter 6
  SOL14998 - BIG-IP APM access policy ACLs and network access tunnels
  SOL13515 - Support for Access Control Lists in tunnel to tunnel connections

Objective 2.19: Describe methods to map Microsoft Active Directory groups to assigned resources
- Configuring BIG-IP APM, Chapter 10
  SOL12193 - Using nested groups in Active Directory for authentication and resource assignment

Objective 2.20: Explain the use of APM session variables (e.g., session flow, use in iRules, variable assign policy item)
Determine which Use the iRule event policy item in the VPE
Determine the appropriate Access Policy modifications to meet specific authentication requirements
- Configuring BIG-IP APM, Chapter 12
  SOL13417 - Using session variables in resource objects (11.x)
Objective 2.21: Explain access policy flow and logic (i.e., branching, loops, macros [when and how to use them])
- Configuring BIG-IP APM, Chapters 3 and 10

Objective 2.22: Describe the use and configuration of endpoint checks (e.g., registry check, process check, Windows info, machine cert auth)
Configure endpoint checks: AV check, registry check, file check, firewall check, process check, machine certification check
- SOL13614 - Overview of the access policy Machine Cert Auth action

Determine which steps are necessary to add macro checks to a policy
Determine which steps are necessary to take when adding authentication methods
- Configuring BIG-IP APM, Chapters 11 and 12

Objective 2.23: Describe customization options for an access policy (logon page, webtop, network access, language)
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)
Configuring BIG-IP APM, Chapters 3, 5, 7, 11, and 12

- SOL15087 - Adding a custom image for the BIG-IP APM access profile login page

Section 3: Maintain APM access profiles

Objective 3.01: Interpret device performance information (e.g., dashboard, statistics tab, ACL denied report)
- Configuring BIG-IP APM, Chapters 2, 6, 9 and 10
  - Customizing the BIG-IP Dashboard

Objective 3.02: Identify necessary software maintenance procedures to address a given condition
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

© 2013 F5 Networks, Inc.
Describe what happens during an upgrade if an active APM device was to failover to standby

SOL10942 - Installing OPSWAT hotfixes on BIG-IP APM systems
SOL12385 - OPSWAT support chart
SOL14207 - Determining the active OPSWAT version
SOL15000 - Using the Automatic Update Check feature

Objective 3.03: Determine how upgrades on production systems affect end users (e.g., client components and high availability failover)

Section 4: Identify and resolve APM issues

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)

- Configuring BIG-IP APM, Chapters 5 and 7
  SOL14045 - The BIG-IP Edge Client components for Windows
  SOL12444 - Overview of the Component Troubleshooting Utility
  SOL14947 - The BIG-IP Edge Client components for Mac OS X
  SOL14782 - BIG-IP APM support for the Windows 8.1 operating system and Internet Explorer 11
  SOL9694 - Overview of the Windows DNS Relay Proxy service

Objective 4.02: Interpret client and machine certificates (e.g., subject, issuer)
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)
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., SS LDump and TCPDump)
Perform and interpret output of TCPDump
Determine the correct TCPDump and SS LDump to resolve specific issues

SOL11898: Information required when opening a support case for BIG-IP APM
SOL4714: Performing a packet trace and providing the results to F5 Technical Support
SOL10209 - Overview of packet tracing with the ssldump utility

© 2013 F5 Networks, Inc.
Objective 4.05: Analyze and interpret APM-specific log files (e.g., APM, SSO, rewrite)

Identify error messages in log file outputs

Determine the root cause of login issues based on information provided in log files

- Configuring BIG-IP APM, Chapter 10
  SOL13394 - Overview of BIG-IP APM logging destinations
  SOL13455: Overview of BIG-IP logging BigDB database keys (11.x)

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)

Locate error codes

List and describe APM logging services

Locate core files

- Configuring BIG-IP APM, Chapters 5, 10 and 12
  SOL11308 - Overview of the adtest tool
  SOL11134 - Locating a user’s session ID
  SOL13384 - Performing a web applications trace (11.x)
  SOL9311 - Best Practices for LDAP Monitoring

Objective 4.07: Diagnose and resolve authentication issues (e.g., client>APM, APM>AAA, APM>SSO)

Analyze http requests to determine authentication issues

SOL13510 - Overview of the Kerberos SSO GSSAPI header

Objective 4.08: Diagnose and resolve client side issues related to connections, performance, and endpoint inspection

Determine the root cause of authentication and client side issues

Differentiate between different types of authentication and client side issues