Download Zscaler ZDTA Exam Dumps Free

Shared by Mcdonald on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Is SCIM required for ZIA?

Options:

A- Depends
B- Maybe
C- No
D- Yes

Answer:

C

Explanation:

SCIM is optional for ZIA user provisioning - you can onboard users via manual CSV import, SAML attributes, or other identity integrations without implementing SCIM.

Question 2

Question Type: MultipleChoice

What method does Zscaler Identity Threat Detection and Response use to gather information about AD domains?

Options:

A- Scanning network ports
B- Running LDAP queries
C- Analyzing firewall logs
D- Packet sniffing

Answer:

B

Explanation:

Zscaler Identity Threat Detection and Response gathers information about Active Directory (AD) domains primarily by running LDAP queries. LDAP queries allow the system to retrieve user and domain information directly and accurately from the AD infrastructure, enabling detection and analysis of identity threats and suspicious activities.

The study guide highlights the use of LDAP queries as a reliable and standard method for accessing AD domain data in this security context.

Question 3

Question Type: MultipleChoice

The security exceptions allow list for Advanced Threat Protection apply to Which option best Policies?

Options:

A- Sandbox
B- URL Filtering
C- File Type Control
D- IPS Control

Answer:

A

Explanation:

The ATP ''Security Exceptions'' allow list is leveraged by both Advanced Threat Protection and the Sandbox policy - URLs or hosts you add here won't be submitted for sandbox analysis.

Question 4

Question Type: MultipleChoice

Which Risk360 key focus area observes a broad range of event, security configurations, and traffic flow attributes?

Options:

A- External Attack Surface
B- Prevent Compromise
C- Data Loss
D- Lateral Propagation

Answer:

B

Explanation:

Prevent Compromise analyzes device and network telemetry - including security configurations, event logs, and traffic flows - to gauge how well you're blocking initial intrusion attempts and misconfigurations.

Question 5

Question Type: MultipleChoice

When users are authenticated using SAML, what are the two most efficient ways of provisioning the users?

Options:

A- Hosted User Database and Directory Server Synchronization
B- SAML and Hosted User Database
C- SCIM and Directory Server Synchronization
D- SCIM and SAML Autoprovisioning

Answer:

D

Explanation:

The two most efficient ways to provision users authenticated via SAML are SCIM (System for Cross-domain Identity Management) and SAML Autoprovisioning. SCIM allows automated user provisioning and deprovisioning, while SAML Autoprovisioning enables dynamic user account creation upon authentication, streamlining user lifecycle management.

Question 6

Question Type: MultipleChoice

How would an administrator retrieve the access token to use the Zscaler One API?

Options:

A- The administrator needs to send a POST request along with the required parameters to ZIdentity's token endpoint.
B- The administrator needs to send a GET request along with the required parameters to ZIdentity's token endpoint.
C- The administrator needs to logon to the ZIA portal to generate the access token with Super Admin role.
D- The administrator needs to logon to the ZIA portal to generate the access token with API Admin role.

Answer:

A

Explanation:

You obtain the Zscaler One API access token by sending a POST request with your client_id, client_secret (and any other required parameters) to ZIdentity's OAuth2 token endpoint, which then returns a JWT you use for subsequent API calls.

Question 7

Question Type: MultipleChoice

When configuring Zscaler Private Access, what is the function of the Server Group?

Options:

A- Maps FQDNs to IP Addresses
B- Maps Applications to FQDNs
C- Maps App Connector Groups to Application Segments
D- Maps Applications to Application Groups

Answer:

A

Explanation:

A Server Group holds the actual backend endpoints - defined by FQDNs (or IPs) and ports - and effectively maps those FQDNs to their IP addresses so ZPA knows which hosts to steer traffic toward.

Question 8

Question Type: MultipleChoice

Which filtering policy blocked access to the Network Application?

Options:

A- Sandbox
B- Browser Control
C- Firewall Filtering
D- DLP

Answer:

C

Explanation:

Firewall Filtering policies govern network level application traffic, so access to a Network Application is blocked by a Firewall Filtering rule.

Question 9

Question Type: MultipleChoice

Malware Protection inside HTTPS connections is performed using which parts of the Zero Trust Exchange?

Options:

A- Deception creating decoy files for malware to discover.
B- Application Segmentation of users to specific private applications.
C- TLS Inspection decrypting traffic to compare signatures for known risks.
D- Data Loss Protection comparing saved filenames for known risks.

Answer:

C

Explanation:

Malware Protection for HTTPS traffic relies on the Zero Trust Exchange's TLS Inspection to decrypt the SSL/TLS stream, enabling the malware detection engines to scan payloads against known threat signatures.