Vendor: Zscaler

Exam Code: ZDTA

Exam Name: Zscaler Digital Transformation Administrator

Version: DEMO

QUESTION 1
Assume that you have four data centers around the globe, each hosting multiple applications for your users. What is the minimum number of App Connectors you should deploy?

A. Six – one per data center plus two for cold standby.
B. Eight – two per data center.
C. Four – one per data center.
D. Sixteen – to support a full mesh to the other data centers.

Answer: B
Explanation:
You need at least two App Connectors per data center to ensure high availability and load distribution, so with four data centers the minimum total is eight.

QUESTION 2
When are users granted conditional access to segmented private applications?

A. After passing criteria checks related to authorization and security.
B. Immediately upon connection request for best performance.
C. After a short delay of a random number of seconds.
D. After verifying the user password inside of private application.

Answer: A
Explanation:
Users receive conditional access only once they satisfy the policy's authorization and security criteria, ensuring device posture, user identity, and any other checks have passed before they can reach the segmented application.

QUESTION 3
What mechanism identifies the ZIA Service Edge node that the Zscaler Client Connector should connect to?

A. The PAC file used in the Forwarding Profile
B. The PAC file used in the Application Profile
C. The IP ranges included/excluded in the App Profile
D. The Machine Key used in the Application Profile

Answer: A
Explanation:
Zscaler Client Connector retrieves the Proxy Auto-Config (PAC) file defined in its Forwarding Profile, and that PAC file contains the logic, based on geolocation, network conditions, and other parameters, to direct the client to the optimal ZIA Service Edge node.

QUESTION 4
Zscaler forwards the server SSL/TLS certificate directly to the user's browser session in which situation?

A. When traffic contains a known threat signature.
B. When web traffic is on custom TCP ports.
C. When traffic is exempted in SSL Inspection policy rules.

D. When user has connected to server in the past.

Answer: C
Explanation:
When a connection matches an SSL Inspection rule set to “bypass,” Zscaler performs a passthrough, simply relaying the origin server’s certificate intact to the client rather than substituting its own.

QUESTION 5
What conditions can be referenced for Trusted Network Detection?

A. Hostname Resolution, Network Adapter IP, Default Gateway
B. DNS Servers, DNS Search Domain, Network Adapter IP
C. Hostname Resolution, DNS Servers, Geo Location
D. DNS Search Domain, DNS Server, Hostname Resolution

Answer: D
Explanation:
Trusted Network Detection in Zscaler Client Connector can reference DNS Search Domains, DNS Server IPs, and Hostname Resolution (i.e. a hostname and the IP it resolves to) as criteria for determining a trusted network.

QUESTION 6
Which of the following DLP components make use of Boolean Logic?

A. DLP Identifiers
B. DLP Engines
C. DLP Dictionaries
D. DLP Rules

Answer: B
Explanation:
A DLP engine is defined by a logical expression that combines one or more DLP dictionaries using Boolean operators (All/AND, Any/OR, Exclude/NOT, Sum), making engines the component that leverages Boolean logic.

QUESTION 7
What does the user risk score enable a user to do?

A. Configure stronger user-specific policies to monitor & control user-level risk exposure.
B. Determine if a user has been compromised
C. Determine whether or not a user is authorized to view unencrypted data.
D. Compare the user risk score with other companies to evaluate users vs other companies.

Answer: A
Explanation:
The User Risk Score quantifies each user’s security posture based on their behaviors, enabling administrators to drive dynamic, per-user access control policies--such as tighter URL filtering or application restrictions -- tailored to individual risk levels.

Reference:

https://www.zscaler.com/blogs/product-insights/how-zscaler-s-dynamic-user-risk-scoring-works

QUESTION 8
Cross-Site Scripting (XSS) Protection can protect you against which two types of exploits?

A. Security Exceptions and Malicious Active Content Protection
B. File Format Vulnerabilities and Browser Exploits
C. Cookie Stealing and Potentially Malicious Requests
D. Cookie Stealing and Advanced Threats Policy

Answer: C
Explanation:
Zscaler's Cross-Site Scripting Protection component blocks attempts at session cookie harvesting ("Cookie Stealing") and any injected or obfuscated script payloads sent as "Potentially Malicious Requests."

Reference:
https://www.zscaler.com/resources/white-papers/intrusion-prevention.pdf

QUESTION 9
An organization has more than one ZIA instance, each on different clouds. The organization is using the same login domain for both and upon login Users are given this menu in ZCC asking which cloud they would like to join. What steps could an Administrator take to avoid having this menu appear?

A. Create only one SAML integration with the desired ZIA instance.
B. Customize an MSI version of the ZCC file specifying the USERDOMAIN variable.
C. Customize an MSI version of the ZCC file specifying the CLOUDNAME variable.
D. Federate the login domain between two different IDP instances.

Answer: C
Explanation:
Embedding the CLOUDNAME in the installer binds the Connector to that specific ZIA instance, so users won't be prompted to choose between clouds at login.

QUESTION 10
What method does Zscaler Identity Threat Detection and Response use to gather information about AD domains?

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

Answer: B
Explanation:
Zscaler's Identity Threat Detection and Response continuously audits your Active Directory by issuing LDAP queries against the domain controllers to enumerate schema, users, objects, and computers -- enabling real-time visibility into AD configurations and permissions.

Reference:

https://help.zscaler.com/itdr/what-zscaler-itdr

QUESTION 11
When configuring Webhook alerts in ZIA, what are the two Webhook authentications types supported?

A. Basic and OAuth
B. Token and OAuth
C. Basic and Token
D. Digest and OAuth

Answer: C
Explanation:
When you configure Webhook alerts in Zscaler Internet Access, the only two authentication methods you can choose are Basic (username/password) and Token (API token).

Reference:
https://help.zscaler.com/zia/adding-webhook

QUESTION 12
Which of the following is unrelated to the properties of 'Trusted Networks'?

A. Network Range
B. Org ID
C. Default Gateway
D. DNS Server

Answer: B
Explanation:
Trusted Networks in Zscaler are defined by network attributes such as Network Range, Default Gateway, DNS Server, DHCP Server, and similar static properties to identify on-net locations. The Org ID is a global tenant identifier and isn't a per-network property.

Reference:
https://help.zscaler.com/zscaler-client-connector/searching-trusted-network

QUESTION 13
What is the purpose of the Zscaler Client Connector providing the authentication token to the Zscaler Client Connector Portal after it is received from Zscaler Internet Access?

A. To share the authentication token with the SAML IdP to validate the user session
B. To immediately grant the user access to Zscaler Private Access resources
C. To bypass multifactor authentication (MFA) during the enrollment process
D. To enable the portal to register the user's device and pass the registration to Zscaler Internet Access

Answer: D
Explanation:
Once Zscaler Internet Access validates the SAML assertion, it returns an authentication token to the Client Connector. The Connector then forwards this token to the Zscaler Client Connector Portal so that the portal can register (or update) the device's record. After registration, the portal

passes the necessary device-identity information back to ZIA, completing the enrollment and ensuring subsequent traffic is correctly attributed to that device.

Reference:
https://help.zscaler.com/zscaler-client-connector/using-zscaler-client-connector-portal-identity-provider

QUESTION 14
Which of the following provides for the discovery of Newly Observed Domains within 3 minutes of the domain coming online?

A. IP Chicken
B. MX Toolbox
C. Farsight Feed
D. Dig

Answer: C
Explanation:
The Farsight “Newly Observed Domains” (NOD) feed provides near real-time visibility into domains as soon as they first resolve on the Internet -- typically within 60 seconds (well under three minutes) of appearing in DNS. Other tools like dig or MX Toolbox rely on manual queries and aren’t designed for continuous, automated discovery.

Reference:
https://www.cdw.com/product/farsight-security-newly-observed-domains-subscription-license-1-year/6695376

QUESTION 15
An administrator wants to allow users to access a wide variety of untrusted URLs. Which of the following would allow users to access these URLs in a safe manner?

A. App connector
B. Browser Isolation
C. Zscaler Private Access
D. Zscaler client connector

Answer: B
Explanation:
Zscaler Browser Isolation safely streams untrusted web content as pixels from a cloud sandbox -- separating users from active page elements and malware -- so users can access a wide variety of risky or uncategorized URLs without exposing their devices or network.

Reference:
https://www.zscaler.com/resources/security-terms-glossary/what-is-remote-browser-isolation

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**