FreeCram

FreeCram

Instant Download | 365 Days Free Updates | Money Back Guarantee | Security & Privacy

Full refund if you fail the corresponding exam in 60 days after purchasing. And Free get any another product.

We're not the only ones **happy** about FreeCram Practice Material ...

12514+ customers in 100+ countries use FreeCram Test Engine. Meet our customers.

https://www.freecram.com

Free Exam/Cram Practice Materials.

Exam : **NSK101**

Title : Netskope Certified Cloud Security Administrator

Vendor : Netskope

Version : DEMO

NO.1 Which Netskope component would an administrator use to see an overview of private application usage and performance?

A. Digital Experience Management

B. Publishers page

C. Incident Management

D. Cloud Exchange

Answer: A

Explanation:

An administrator would use the Digital Experience Management (DEM) component to see an overview of private application usage and performance. DEM provides comprehensive insights into the performance and user experience of private applications, including metrics on latency, bandwidth, and application health.

* Digital Experience Management (DEM): This component focuses on monitoring and optimizing the user experience for private and public applications by collecting detailed performance data and providing actionable insights.

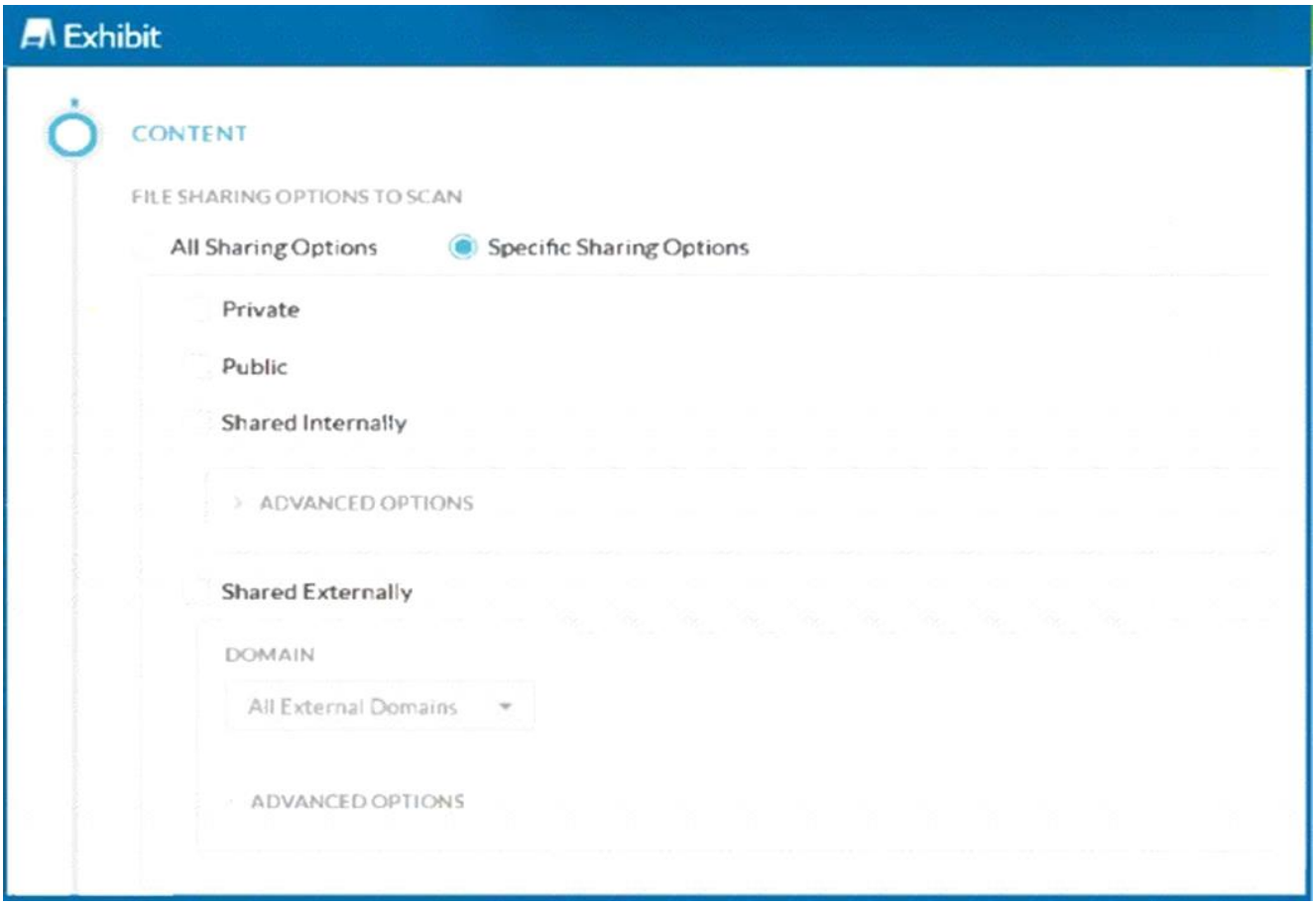
The other options do not provide the same level of detailed performance and usage overview for private applications:

* Publishers page: Typically used for managing and configuring Netskope Publishers.
* Incident Management: Focuses on tracking and resolving security incidents.
* Cloud Exchange: Deals with integrations and data sharing between Netskope and other security solutions.

References:

* Netskope documentation on Digital Experience Management and its capabilities.
* Best practices for using DEM to monitor application performance and enhance user experience.

NO.2 Click the Exhibit button.



A customer has created a CASB API-enabled Protection policy to detect files containing sensitive data that are shared outside of their organization.
Referring to the exhibit, which statement is correct?

A. The administrator needs to use Shared Externally as the only shared option.

B. The administrator needs to use Shared Externally and Public as the shared options.

C. The administrator must select Private as the only shared option.

D. The administrator needs to use Public as the only shared option.

Answer: B

Explanation:

To detect files containing sensitive data that are shared outside of the organization, the administrator should select both "Shared Externally" and "Public" sharing options. These settings ensure that any files shared externally (outside the organization) or publicly are scanned for sensitive data. This comprehensive approach covers all potential scenarios where data could be exposed outside the organization.

Step-by-Step Configuration:

* Select Specific Sharing Options:
* Navigate to the CASB API-enabled Protection policy configuration page.
* Choose the option for "Specific Sharing Options" to limit the scan to files shared under certain conditions.
* Enable Shared Externally and Public:
* Check both "Shared Externally" and "Public" options. This setting ensures that files shared either publicly or with external domains are included in the scan.
* Configure Advanced Options:

* For further granularity, configure the advanced options under each sharing type if needed (e.g., specifying particular external domains).
This configuration aligns with the best practices for CASB policies and ensures that all files potentially leaving the organization are scanned for sensitive data.
References:
* Netskope CASB Policy Configuration Documentation

NO.3 What are two valid use cases for the Cloud Confidence Index (CCI)? (Choose two.)

A. To recategorize cloud applications in the database

B. To delete cloud applications from the database

C. To identify the activities that Netskope supports for cloud applications

D. To compare similar cloud applications

Answer: C D

Explanation:
The Cloud Confidence Index (CCI) has several use cases, including:
* To identify the activities that Netskope supports for cloud applications: The CCI helps administrators understand which activities are supported and monitored by Netskope for various cloud applications. This includes knowing the types of data that can be protected and the actions that can be controlled within those applications.
* To compare similar cloud applications: The CCI provides a comparative assessment of cloud applications based on their security and compliance postures. This allows organizations to make informed decisions about which applications to approve or restrict based on their confidence levels.
These use cases help organizations enhance their security posture by using the CCI to guide application usage policies and ensure compliance with internal standards.
References:
* Netskope documentation on Cloud Confidence Index and its applications in policy creation and management.
* Guides on using CCI to assess and compare cloud applications for better security and compliance.

NO.4 You are deploying TLS support for real-time Web and SaaS transactions. What are two secure implementation methods in this scenario? (Choose two.)

A. Bypass TLS 1.3 because it is not widely adopted.

B. Downgrade to TLS 1.2 whenever possible.

C. Support TLS 1.2 only when 1.3 is not supported by the server.

D. Require TLS 1.3 for every server that accepts it.

Answer: C D

Explanation:
If you are deploying TLS support for real-time Web and SaaS transactions, then you need to use secure implementation methods that ensure the highest level of encryption and security for your traffic. Two secure implementation methods in this scenario are: support TLS 1.2 only when 1.3 is not supported by the server and require TLS 1.3 for every server that accepts it. TLS stands for Transport Layer Security, which is a protocol that provides secure communication over the internet by encrypting and authenticating data exchanged between two parties. TLS 1.3 is the latest version of TLS, which offers several improvements over TLS 1.2, such as faster handshake, stronger encryption algorithms, better forward secrecy, and reduced attack surface.

Therefore, it is recommended to use TLS 1.3 whenever possible for real-time Web and SaaS transactions, as it provides better security and performance than TLS 1.2. However, some servers may not support TLS 1.3 yet, so in those cases, it is acceptable to use TLS 1.2 as a fallback option, as it is still considered secure and widely adopted. Bypassing TLS 1.3 because it is not widely adopted or downgrading to TLS 1.2 whenever possible are not secure implementation methods in this scenario, as they would compromise the security and performance of your traffic by using an older or weaker version of TLS than necessary. References: [TLS],
[TLS 1.3].

NO.5 Which statement is correct about Netskope's Instance Awareness?

A. It prevents users from browsing the Internet using outdated Microsoft Internet Explorer but allows them access if they use the latest version of Microsoft Edge.

B. It identifies that a form hosted in Microsoft Forms belongs to the corporate Microsoft 365 tenant and not a tenant from a third party.

C. It differentiates personal code from work-related code being uploaded to GitHub.

D. It identifies if e-mails are being sent using Microsoft 365 through Outlook, Thunderbird, or the Web application in outlook.com.

Answer: B

Explanation:
Instance Awareness in Netskope provides visibility and control over instances of applications used by the organization. Specifically, it helps in differentiating between corporate and personal instances of the same application. This feature is particularly crucial in ensuring that corporate data is not uploaded to personal instances of applications and vice versa.
For example, it can identify that a form hosted in Microsoft Forms belongs to the corporate Microsoft 365 tenant, thereby preventing data from being mistakenly or maliciously sent to a third-party tenant. This ensures that only authorized instances of applications are used for corporate data, maintaining data security and compliance.
References:
* Using the REST API v2 UCI Impact Endpoints - Netskope Knowledge Portal
* REST API v2 Overview - Netskope Knowledge Portal
* Using the REST API v2 dataexport Iterator Endpoints - Netskope Knowledge Portal

NO.6 Which Netskope platform component uses NewEdge Traffic Management for traffic steering?

A. Cloud Exchange

B. Client

C. Data Plane On-Premises

D. Explicit Proxy Over Tunnel

Answer: B

Explanation:
NewEdge Traffic Management:
* NewEdge is Netskope's high-performance global network designed to deliver fast and secure access to the internet and cloud applications.
* NewEdge Traffic Management ensures efficient routing and traffic steering for optimal performance and security.
Client Integration:

* The Netskope Client uses NewEdge Traffic Management to steer traffic securely to the Netskope cloud.
* It ensures that user traffic is routed through the best possible path for performance and security.
* The Client component is responsible for redirecting user traffic to the NewEdge network, applying security policies, and ensuring secure access.
References:
* For detailed information on NewEdge Traffic Management and how the Netskope Client utilizes it, refer to the Netskope documentation on traffic management and client configuration.

NO.7 You are adding a new tenant administrator in the Admins page. Which additional security measure would you be able to enable for only this new account?
A. Activate SSO authentication using an external identity provider.
B. Activate MFA to log in to the Netskope management console.
C. Set the password expiration.
D. Add the administrator to the Administration Audit Log.
Answer: B
Explanation:
When adding a new tenant administrator in the Admins page, you can enhance the security for the new account by enabling Multi-Factor Authentication (MFA). MFA adds an extra layer of security by requiring the administrator to provide a second form of verification in addition to the password, thus protecting against unauthorized access.
References:
* Netskope documentation on user and admin account management, including the configuration and benefits of enabling MFA.
* Security best practices guides from Netskope, emphasizing the importance of MFA for enhanced account security.

NO.8 What correctly defines the Zero Trust security model?
A. least privilege access
B. multi-layered security
C. strong authentication
D. double encryption
Answer: A
Explanation:
The term that correctly defines the Zero Trust security model is least privilege access. The Zero Trust security model is a modern security strategy based on the principle: never trust, always verify. Instead of assuming everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originates from an open network. One of the core principles of the Zero Trust model is to use least privilege access, which means granting users or systems only the minimum level of access they need to perform their tasks, and only for a limited time. This helps reduce the attack surface and minimize the impact of a potential breach. References: Zero Trust Security - microsoft.comWhat is Zero Trust Security?
Principles of the Zero Trust Model

NO.9 You want to determine which NewEdge data planes that your remote users have been recently

using.
Which area of the Netskope Tenant UI would provide this information?
A. Client Steering under Digital Experience Management
B. Network Steering under Digital Experience Management
C. Users page under Settings
D. Devices page under Settings
Answer: A
Explanation:
NewEdge Data Planes Monitoring:
* To determine which NewEdge data planes your remote users have been using, you need to access the relevant monitoring section in the Netskope Tenant UI.
Client Steering under Digital Experience Management:
* The Client Steering section under Digital Experience Management provides detailed information on how traffic is being steered for remote users.
* This section includes insights into the NewEdge data planes being utilized by users.
Steps:
* Navigate to Digital Experience Management in the Netskope Tenant UI.
* Select Client Steering to view detailed reports and logs on traffic steering.
* Analyze the data to identify the NewEdge data planes used by remote users recently.
References:
* For more details on accessing and using the Client Steering section under Digital Experience Management, refer to the Netskope documentation on digital experience management and client steering.

NO.10 As an administrator, you are investigating an increase in the number of incidents related to compromised credentials. You are using the Netskope Compromised Credentials feature on your tenant to assess the situation. Which insights would you find when using this feature? (Choose two)
A. Compromised usernames
B. Breach information source
C. Compromised passwords
D. Affected managed applications
Answer: A B
Explanation:
When using the Netskope Compromised Credentials feature, administrators can gain valuable insights into security incidents related to compromised credentials. The insights provided by this feature include:
* Compromised usernames: This information helps identify which user accounts have been compromised, allowing administrators to take necessary actions such as resetting passwords and notifying affected users.
* Breach information source: Netskope provides details on the source of the breach, such as which third-party service or data breach resulted in the compromise of credentials. This helps in understanding the context of the breach and implementing measures to prevent future incidents.
While compromised passwords (option C) are indirectly involved, they are not explicitly listed as an insight provided by this feature. Similarly, affected managed applications (option D) are related but not directly part of the primary insights.

References:
* Netskope documentation on Compromised Credentials feature and incident response.
* Security best practices for managing and mitigating compromised credential incidents.

NO.11 Your customer has cloud storage repositories containing sensitive files of their partners, including bank statements, consulting, and disclosure agreements. In this scenario, which feature would help them control the flow of these types of documents?

A. ZTNA

B. Netskope Advanced Analytics

C. DLP document classifiers

D. Sandboxing

Answer: C

Explanation:
Data Loss Prevention (DLP) document classifiers are designed to identify and control the flow of sensitive information based on predefined patterns and criteria. In this scenario, where the customer has cloud storage repositories containing sensitive files such as bank statements, consulting agreements, and disclosure agreements, DLP document classifiers can help:
* Identify sensitive documents: By scanning and classifying documents based on their content, DLP document classifiers ensure that sensitive files are recognized and handled appropriately.
* Control data flow: Policies can be applied to prevent unauthorized access, sharing, or movement of sensitive files, thereby protecting the data from leakage or exposure.
References:
* Netskope DLP documentation, detailing how document classifiers work and how they can be configured to protect sensitive information.
* Best practices for implementing DLP solutions to safeguard sensitive data in cloud storage environments.

NO.12 You have an issue with the Netskope client connecting to the tenant.
In this scenario, what are two ways to collect the logs from the client machine? (Choose two.)

A. from the Netskope client UI About page

B. from the command line using the nsdiag command

C. from the Netskope client system tray icon

D. from the Netskope client UI Configuration page

Answer: A B

Explanation:
To collect the logs from the client machine when you have an issue with the Netskope client connecting to the tenant, two ways that you can use are: from the Netskope client UI About page and from the command line using the nsdiag command. From the Netskope client UI About page, you can click on the "Collect Logs" button to generate a zip file containing all the relevant logs and configuration files from the client machine.
You can then send this zip file to Netskope support for troubleshooting. From the command line, you can use the nsdiag command with various options to collect different types of logs and diagnostic information from the client machine. For example, you can use nsdiag -l to collect all logs, nsdiag -c to collect configuration files, nsdiag -t to collect traffic statistics, etc. You can also use nsdiag -h to see all available options and usage instructions. You can then send the output files to Netskope support for

troubleshooting. References: Netskope Client Configuration overviewInstall and Test the Client - Netskope Knowledge Portal

NO.13 Which networking function does a SASE solution provide above and beyond an SSE solution?

A. Secure Web Gateway

B. Cloud Access Security Broker

C. Data Loss Prevention

D. Software Defined Wide Area Network

Answer: D

Explanation:

A SASE (Secure Access Service Edge) solution provides networking functions that go beyond the capabilities of an SSE (Security Service Edge) solution. Specifically, a SASE solution integrates:

* Software Defined Wide Area Network (SD-WAN): SD-WAN enhances network performance and efficiency by dynamically routing traffic across the best available paths. It provides greater flexibility, improved application performance, and reduced costs compared to traditional WAN solutions.

In contrast, SSE focuses on security services like Secure Web Gateway, Cloud Access Security Broker, and Data Loss Prevention, but does not include networking functions such as SD-WAN.

References:

* Netskope's documentation on SASE and SSE solutions, highlighting the differences and additional functionalities provided by SASE, including SD-WAN.
* Detailed explanation of SD-WAN and its integration into SASE solutions.