Free Questions for NSK101 by dumpssheet

Shared by Guy on 11-03-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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.)

Options:

A- from the Netskope client Ul About page

B- from the command line using the nsdiag command

C- from the Netskope client system tray icon

D- from the Netskope client Ul 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.Reference:Netskope Client Configuration overviewInstall and Test the Client - Netskope Knowledge Portal

Question 2

Question Type: MultipleChoice

When would an administrator need to use a tombstone file?

Options:

A- You use a tombstone file when a policy causes a file download to be blocked.

B- You use a tombstone file when a policy causes a publicly shared file to be encrypted.

C- You use a tombstone file when the policy causes a file to be moved to quarantine.

D- You use a tombstone file when a policy causes a file to be moved to legal hold.

Answer:

C

Explanation:

A tombstone file is a placeholder file that replaces the original file when it is moved to quarantine by a Netskope policy. The tombstone file contains information about the original file, such as its name, size, type, owner, and the reason why it was quarantined. The tombstone file also provides a link to the Netskope UI where the administrator or the file owner can view more details about the incident and take appropriate actions, such as restoring or deleting the file. The purpose of using a tombstone file is to preserve the metadata and location of the original file, as well as to notify the users about the quarantine action and how to access the file if needed.Reference:Threat Protection - Netskope Knowledge PortalNetskope threat protection - Netskope

Question 3

Question Type: MultipleChoice

How do you provision users to your customer's Netskope tenant? (Choose two.)

Options:

A- Use Microsoft Intune.

B- Use the AD Connector.

C- Use SCIM.

D- Use the Directory Importer.

Answer:

B, D

Explanation:

To provision users to your customer's Netskope tenant, two methods that you can use are: use the AD Connector and use SCIM. The AD Connector is a tool that allows you to synchronize users and groups from your Active Directory (AD) domain to your Netskope tenant. The AD Connector runs as a Windows service on a machine that has access to your AD domain controller. The AD Connector periodically queries your AD domain for any changes in users and groups and updates them in your Netskope tenant accordingly. The AD Connector also supports filtering users and groups based on attributes or organizational units (OUs). SCIM stands for System for Cross-domain Identity Management, which is a standard protocol for managing user identities across different applications and services. SCIM allows you to provision users and groups from your identity provider (IdP), such as Azure AD or Okta, to your Netskope tenant using APIs. SCIM also supports creating, updating, deleting, and searching users and groups in your Netskope tenant based on your IdP's configuration.Reference:Netskope AD ConnectorUser Provisioning with Azure AD

Question 4

Question Type: MultipleChoice

You want to block access to sites that use self-signed certificates. Which statement is true in this scenario?

Options:

A- Certificate-related settings apply globally to the entire customer tenant.

B- Certificate-related settings apply to each individual steering configuration level.

C- Certificate-related settings apply to each individual client configuration level.

D- Self-signed certificates must be changed to a publicly trusted CA signed certificate.

Answer:

B

Explanation:

The statement that is true in this scenario is: Certificate-related settings apply to each individual steering configuration level. Certificate-related settings are the options that allow you to configure how Netskope handles SSL/TLS certificates for encrypted web traffic. For example, you can choose whether to allow or block self-signed certificates, expired certificates, revoked certificates, etc. You can also choose whether to enable SSL decryption for specific domains or categories. Certificate-related settings apply to each individual steering configuration level, which means that you can have different settings for different types of traffic or devices. For example, you can have one steering configuration for managed devices and another one for unmanaged devices, and apply different certificate-related settings for each one. This allows you to customize your security policies based on your needs and preferences.Reference:Netskope SSL DecryptionNetskope Steering Configuration

Question 5

Question Type: MultipleChoice

When using an out-of-band API connection with your sanctioned cloud service, what are two capabilities available to the administrator? (Choose two.)

Options:

A- to quarantine malware

B- to find sensitive content

C- to block uploads

D- to allow real-time access

Answer:

A, B

Explanation:

When using an out-of-band API connection with your sanctioned cloud service, two capabilities available to the administrator are: to quarantine malware and to find sensitive content. An out-of-band API connection is a method of integrating Netskope with your cloud service provider using the APIs exposed by the cloud service. This allows Netskope to access the data that is already stored in the cloud service and perform retrospective inspection and enforcement of policies. One capability that the administrator can use with an out-of-band API connection is to quarantine malware. This means that Netskope can scan the files in the cloud service for malware, ransomware, phishing, and other threats, and move them to a quarantine folder or delete them if they are found to be malicious. Another capability that the administrator can use with an out-of-band API connection is to find sensitive content. This means that Netskope can scan the files in the cloud service for sensitive data, such as personal information, intellectual property, or regulated data, and apply data loss prevention (DLP) policies to protect them. For example, Netskope can encrypt, redact, or watermark the files that contain sensitive content, or notify the administrator or the file owner about the exposure.Reference:Netskope API ProtectionReal-time Control and Data Protection via Out-of-Band API

Question 6

Question Type: MultipleChoice

You want to set up a Netskope API connection to Box.

What two actions must be completed to enable this connection? (Choose two.)

Options:

A- Install the Box desktop sync client.

B- Authorize the Netskope application in Box.

C- Integrate Box with the corporate IdP.

D- Configure Box in SaaS API Data protection.

Answer:

B, D

Explanation:

To set up a Netskope API connection to Box, two actions that must be completed are: authorize the Netskope application in Box and configure Box in SaaS API Data protection. Authorizing the Netskope application in Box allows Netskope to access the Box API and perform out-of-band inspection and enforcement of policies on the data that is already stored in Box. Configuring Box in SaaS API Data protection allows you to specify the Box instance details, such as domain name, admin email, etc., and enable features such as retroactive scan, event stream, etc.Reference:Authorize Netskope Introspection App on Box Enterprise - Netskope Knowledge PortalConfigure Box Instance in Netskope UI - Netskope Knowledge Portal