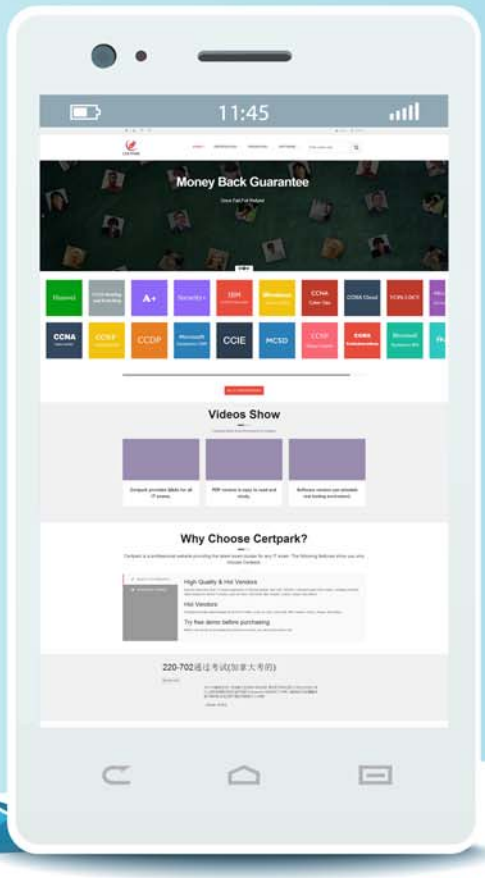
CERTPARK

QUESTION & ANSWER

CERTPARK.COM

Accurate Study Guides,
High Passing Rate!
provides update
free of charge
in one year!



https://www.certpark.com

Exam : **NSK300**

Title : Netskope Certified Cloud Security Architect Exam

Version : DEMO

1.You are asked to create a customized restricted administrator role in your Netskope tenant for a newly hired employee.
Which two statements are correct in this scenario? (Choose two.)
A. An admin role prevents admins from downloading and viewing file content by default.
B. The scope of the data shown in the UI can be restricted to specific events.
C. All role privileges default to Read Only for all functional areas.
D. Obfuscation can be applied to all functional areas.
Answer: AC
Explanation:
Admin Role and File Content Viewing: By default, an admin role does not prevent admins from downloading and viewing file content. Admins have access to view and download file content unless specific restrictions are applied.
Role Privileges Default to Read Only: All role privileges in Netskope default to Read Only for all functional areas. This means that admins can view information but cannot make changes unless explicitly granted additional permissions.
Obfuscation: Obfuscation can be applied to specific functional areas, but it is not a default behavior for all areas.
Reference: Netskope Security Cloud Introductory Online Technical Training
Netskope Security Cloud Operation & Administration (NSCO&A) - Classroom Training

2.You are deploying the Netskope Client to Windows devices.
The following command line would be used to install the client MSI file:

```
msiexec /I NSClient.msi token=<token> host=<host> [mode=peruserconfig | installmode=IDP [userconfiglocation=<path>]] fail-close=[no-npa|all] [autoupdate=on|off]
```

In this scenario, what is <token> referring to in the command line?
A. a Netskope user identifier
B. the Netskope organization ID
C. the URL of the IdP used to authenticate the users
D. a private token given to you by the SCCM administrator
Answer: B
Explanation:
In the context of deploying the Netskope Client to Windows devices, <token> in the command line refers to the Netskope organization ID. This is a unique identifier associated with your organization's account within the Netskope security cloud. It is used during the installation process to ensure that client devices are registered and managed under the correct organizational account, enabling appropriate security policies and configurations to be applied.
Reference: The answer can be inferred from general knowledge about installing software clients and isn't directly available on Netskope's official resources.

3.Given the following:

```
user eq 'user@company.com' and access_method eq 'Client' and activity eq 'Download' or activity eq 'Upload' and site eq 'Amazon S3'
```

Which result does this Skope IT query provide?
A. The query returns all events of user@company.com downloading or uploading to or from the site 'Amazon S3" using the Netskope Client.
B. The query returns all events of an IP address downloading or uploading to or from Amazon S3 using

the Netskope Client.
C. The query returns all events of everyone except user@company.com downloading or uploading to or from the site "Amazon S3" using the Netskope Client.
D. The query returns all events of user@company.com downloading or uploading to or from the application "Amazon S3" using the Netskope Client.
Answer: A
Explanation:
The given Skope IT query specifies the following conditions:
User equals ‘user@company.com’
Access method equals ‘Client’
Activity equals ‘Download’ or ‘Upload’
Site equals ‘Amazon S3’
The query combines these conditions using logical operators (AND and OR).
The result of this query will include all events where the specified user (‘user@company.com’) is either downloading or uploading data to or from the site ‘Amazon S3’ using the Netskope Client. It does not include events related to other users or IP addresses.
Reference: Netskope Security Cloud Introductory Online Technical Training
Netskope Security Cloud Operation & Administration (NSCO&A) - Classroom Training

4.You want customers to configure Real-time Protection policies.
In which order should the policies be placed in this scenario?
A. Threat, CASB, RBI, Web
B. RBI, CASB, Web, Threat
C. Threat, RBI, CASB, Web
D. CASB, RBI, Threat, Web
Answer: B
Explanation:
When configuring Real-time Protection policies in Netskope, the recommended order is as follows: RBI (Risk-Based Index) Policies: These policies focus on risk assessment and prioritize actions based on risk scores. They help identify high-risk activities and users.
CASB (Cloud Access Security Broker) Policies: These policies address cloud-specific security requirements, such as controlling access to cloud applications, enforcing data loss prevention (DLP) rules, and managing shadow IT.
Web Policies: These policies deal with web traffic, including URL filtering, web categories, and threat prevention.
Threat Policies: These policies focus on detecting and preventing threats, such as malware, phishing, and malicious URLs.
Placing the policies in this order ensures that risk assessment and cloud-specific controls are applied before addressing web and threat-related issues.
Reference: Netskope Security Cloud Introductory Online Technical Training
Netskope Security Cloud Operation & Administration (NSCO&A) - Classroom Training
Netskope Certification Description
Netskope Architectural Advantage Features

5.A company has deployed Explicit Proxy over Tunnel (EPoT) for their VDI users They have configured Forward Proxy authentication using Okta Universal Directory They have also configured a number of Real-time Protection policies that block access to different Web categories for different AD groups so. for example, marketing users are blocked from accessing gambling sites. During User Acceptance Testing, they see inconsistent results where sometimes marketing users are able to access gambling sites and sometimes they are blocked as expected They are seeing this inconsistency based on who logs into the VDI server first.
What is causing this behavior?
A. Forward Proxy is not configured to use the Cookie Surrogate
B. Forward Proxy is not configured to use the IP Surrogate
C. Forward Proxy authentication is configured but not enabled.
D. Forward Proxy is configured to use the Cookie Surrogate
Answer: A
Explanation:
The inconsistent results observed during User Acceptance Testing (where marketing users sometimes access gambling sites and sometimes are blocked) are likely due to the configuration of the Forward Proxy.
Cookie Surrogate: The Cookie Surrogate is a mechanism used in Forward Proxy deployments to maintain user context across multiple requests. It ensures that user-specific policies are consistently applied even when multiple users share the same IP address (common in VDI environments). Issue: If the Forward Proxy is not configured to use the Cookie Surrogate, it may lead to inconsistent behavior. When different users log into the VDI server, their requests may not be associated with their specific user context, resulting in varying policy enforcement.
Solution: Ensure that the Forward Proxy is properly configured to use the Cookie Surrogate, allowing consistent policy enforcement based on individual user identities.
Reference: Netskope Security Cloud Operation & Administration (NSCO&A) - Classroom Training Netskope Security Cloud Introductory Online Technical Training Netskope Architectural Advantage Features