Free Questions for ChromeOS-Administrator by ebraindumps

Shared by Cohen on 03-06-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Your customer is deploying ChromeOS devices in their environment and requires those ChromeOS devices to adhere to web filtering via TLS (or SSL) Inspection. What recommendations should you make to your customer in setting up the requirements for ChromeOS devices?

Options:

A- Configure a hostname allowlist, set up a TLS (or SSL) certificate, then verify TLS (or SSL) inspection is working

B- Reach out lo Google Workspace Security and Compliance for tailored configurations for your customer

C- Configure a transparent proxy, set up your allowlist to use * google com. then verify TLS (or SSL) inspection is working

D- ChromeOS devices are preconfigured to adhere to company TLS (or SSL) inspection by default and can therefore be deployed with no additional configuration

Answer:

A

Explanation:

To set up TLS (or SSL) inspection for web filtering on ChromeOS devices, you need to follow these steps:

Configure Hostname Allowlist:Create an allowlist of hostnames (e.g.,*.google.com,*[invalid URL removed]) that should bypass TLS inspection.This ensures that essential services like Google services and your own domain can function properly.

Set up TLS Certificate:Obtain the required TLS/SSL certificate from your web filter provider and install it on your web filter.ChromeOS devices need this certificate to establish a secure connection with the web filter for TLS inspection.

Verify TLS Inspection:Once the configuration is in place,test and verify that TLS inspection is working as expected.This involves checking if the web filter can correctly intercept and decrypt HTTPS traffic for websites not on the allowlist.

Why other options are not correct:

Option B:While reaching out to Google Workspace Security and Compliance can be helpful,it's not the primary step in setting up TLS inspection.The configuration needs to be done on the web filter and ChromeOS devices.

Option C:Transparent proxies are generally not recommended for ChromeOS devices as they can interfere with certain functionalities.While it might work with an allowlist for Google domains,it's not the best practice.

Option D:ChromeOS devices do not come preconfigured to adhere to company TLS inspection.This configuration needs to be set up explicitly by the administrator.

About TLS (or SSL) inspection on ChromeOS devices:https://support.google.com/chrome/a/answer/3504942

Verify TLS (or SSL) inspection works:https://support.google.com/chrome/a/answer/3504943

Question 2

Question Type: MultipleChoice

To allow remote users to securely connect to an internal network, the organization you're supporting is using a VPN. The organization would like you to configure the ChromeOS devices so that the Android VPN clients deployed are automatically configured with the correct hostname. How should you configure this in the Admin Console according to Google best practice?

Options:

A- Download the Android app on a ChromeOS device, add the hostname manually then re-upload the app in the organization's private Google Play Store and deploy it lo all ChromeOS devices

B- Contact the VPN provider and ask them to provide you with a custom installable client with the correct configuration pre-configured Then deploy that installable

C- Add a managed configuration using JSON to the Android app

D- Upload a JSON file with the configuration into the Google Play Store

Answer:

C

Explanation:

This is the most efficient and scalable way to automatically configure Android VPN clients on ChromeOS devices with the correct hostname:

Obtain Configuration:Get the required VPN configuration details (hostname,authentication methods,etc.) from the VPN provider or your organization's network administrator.This configuration is typically in JSON format.

Create Managed Configuration:In the Google Admin console,navigate to Devices > Chrome > Settings > Android Apps > Managed Configurations.

Select the VPN App:Choose the specific Android VPN app you want to configure.

Add JSON Configuration:Paste the JSON configuration into the provided field.Ensure the configuration is valid and accurate.

Save and Deploy:Save the managed configuration and apply it to the desired organizational units (OUs) containing the ChromeOS devices.

This method allows you to centrally manage VPN configurations for Android apps on ChromeOS devices, ensuring consistency and reducing the manual effort required from users.

Question 3

Question Type: **MultipleChoice**

What is the recommended way to provision users from an on-prem Active Directory environment into the Google Admin console?

Options:

A- Upload via CSV

B- Admin SDK Directory API

C- Azure AD Google Cloud/G Suite Connector

D- Google Cloud Directory Sync

Answer:

D

Explanation:

The 'Deprovision' command is specifically designed to remove a ChromeOS device from management policy updates. This means the device will no longer receive updates, configurations, or restrictions pushed from the Google Admin console.

Here's what happens when you deprovision a device:

Policy Removal:All enterprise policies and configurations are removed from the device.

Management Removal:The device is disassociated from the Google Admin console and no longer considered managed.

Data Wipe (Optional):You can choose to wipe the device's data during deprovisioning to ensure no company data remains.

Other options like 'Reset,' 'Disable,' or 'Powerwash' may have different effects:

Reset:Resets the device to factory settings but might not remove management if not done through the Admin console.

Disable:Prevents the user from signing in but doesn't remove policies or management.

Powerwash:Factory resets the device,removing all user data and configurations,including management.

Deprovision a device:https://support.google.com/chrome/a/answer/3523633

Question 4

Question Type: MultipleChoice

Which remote command is required to remove a device from management policy updates?

Options:

A- Deprovision

B- Reset

C- Disable

D- Powerwash

Answer:

A

Explanation:

The 'Deprovision' command is specifically designed to remove a ChromeOS device from management policy updates. This means the device will no longer receive updates, configurations, or restrictions pushed from the Google Admin console.

Here's what happens when you deprovision a device:

Policy Removal:All enterprise policies and configurations are removed from the device.

Management Removal:The device is disassociated from the Google Admin console and no longer considered managed.

Data Wipe (Optional):You can choose to wipe the device's data during deprovisioning to ensure no company data remains.

Other options like 'Reset,' 'Disable,' or 'Powerwash' may have different effects:

Reset:Resets the device to factory settings but might not remove management if not done through the Admin console.

Disable:Prevents the user from signing in but doesn't remove policies or management.

Powerwash:Factory resets the device,removing all user data and configurations,including management.

Deprovision a device:https://support.google.com/chrome/a/answer/3523633

Question 5

Question Type: MultipleChoice

When setting up a Chrome Enterprise trial, what is a benefit of choosing to verify the domain?

Options:

A- Identity management

B- Application management

C- Network management

D- Device management

Answer:

A

Explanation:

When you verify your domain during a Chrome Enterprise trial setup, you establish ownership and control over the domain within Google's systems. This is a crucial step in identity management as it allows you to:

Manage user accounts:Create,edit,and delete user accounts within the domain,ensuring control over who can access company resources.

Apply security policies:Enforce security policies like password requirements,two-factor authentication,and access controls for users within the domain.

Single Sign-On (SSO):Enable seamless and secure single sign-on for users across various Google services and other integrated applications.

By verifying the domain, you essentially gain centralized control over user identities and their access to resources, which is a core aspect of identity management.

Question 6

Question Type: MultipleChoice

You are tasked with converting hundreds of Windows & Mac machines across multiple locations to ChromeOS Flex and enrolling them into the Admin console. The available network bandwidth Is limited at many of the locations and the devices are not currently managed

with any endpoint management system. Which two operations are required to perform the task?

Choose 2 answers

Options:

A- Create a dedicated enrollment account tor each location and place them into the OUs you want the devices enrolled into then enable the 'Place ChromeOS device in user organization' policy and enroll the devices using the respective enrollment account for each location

B- Install the Recovery Tool extension on all devices that are to be converted and follow the step-by-step installer to convert each device directly without the need of USB drives

C- Use PXE boot to load the ChromeOS Flex image onto devices and have them automatically convert across all locations after they're restarted

D- Contact an authorized Zero-Touch Enrollment (ZTE) reseller and share the serial numbers of the devices you're converting and the domain you're enrolling them into to have them pre-provisioned into the Admin console

E- Distribute USB flash drives with the ChromeOS Flex image to the different locations and ask local personnel or a services partner to manually convert each device

Answer:

A, E

Explanation:

Create Dedicated Enrollment Accounts:Create separate enrollment accounts for each location,placing them in the respective OUs where the converted devices should be enrolled.

Enable Policy:Turn on the 'Place ChromeOS device in user organization' policy.This ensures devices are automatically enrolled into the correct OU based on the enrollment account used.

Enroll Devices:Use the dedicated enrollment account for each location to enroll the converted devices.This allows for organized management based on location.

Option E:

Distribute USB Drives:Prepare USB flash drives with the ChromeOS Flex image and distribute them to the different locations.

Manual Conversion:Instruct local personnel or a service partner to manually convert each device using the provided USB drives.This method is suitable when network bandwidth is limited and doesn't rely on existing endpoint management infrastructure.

Reasons for not choosing other options:

Option B:The Recovery Tool is primarily used for creating recovery media for ChromeOS devices,not converting other operating systems.

Option C:PXE boot is a network-based installation method,not ideal for locations with limited bandwidth.

Option D:While zero-touch enrollment (ZTE) streamlines enrollment,it requires pre-provisioning devices with the vendor or reseller,which might not be feasible in this scenario.

By combining options A and E, you can efficiently convert and enroll devices in multiple locations with limited network resources and no existing management systems.

Question 7

Question Type: MultipleChoice

How should you use Chrome Remote Desktop from the Google Admin console to connect a user?

Options:

A- Find the user account and click remote desktop

B- Open Chrome Remote Desktop and type the device serial number

C- Open Chrome Remote Desktop and type the user's user name

D- Find the device and click remote desktop

Answer:

D

Explanation:

To initiate a remote desktop session to a ChromeOS device using the Google Admin console, follow these steps:

Sign in to Google Admin console:Use your administrator credentials.

Navigate to Devices:Go to Devices > Chrome > Devices.

Locate the Device:Find the device you want to connect to using its serial number or other identifying information.

Start Remote Desktop Session:Click on the device and select 'Remote desktop.' This will send a connection request to the user,who must accept it before the session can start.

Question 8

Question Type: MultipleChoice

A customer has a mission-critical workload running on ChromeOS and needs devices configured to reduce ChromeOS changes. How can an admin reduce the risk of an unexpected change in an OS update affecting the customer's entire ChromeOS device domain while maintaining security and minimizing admin workload?

Options:

A- Force auto reboot after update

B- Enable variations

C- Move to a Long-term Support channel

D- Add an update rollout plan

Answer:

D

Explanation:

Update rollout plans in the Google Admin console allow administrators to gradually roll out ChromeOS updates to a subset of devices first. This allows for testing in a controlled environment before deploying to the entire fleet, reducing the risk of unexpected issues impacting all devices.

Steps to add an update rollout plan:

Access Google Admin Console:Sign in with your administrator credentials.

Navigate to Device Management:Go to Devices > Chrome > Settings > Updates.

Create Rollout Plan:Click on 'Add an update rollout plan.'

Select Devices:Choose the specific devices or organizational units (OUs) to include in the initial rollout.

Set Timeline:Define the start and end dates for the rollout.

Save and Apply:Save the plan and apply it to the selected devices.

Question 9

Question Type: MultipleChoice

Your hardware OEM issues a recall for a safety issue. You need to deprovision devices from management before returning to the OEM. They will replace your existing ChromeOS devices with a different model. Which option should you choose when deprovisioning to make sure you can reuse your Chrome Education/Enterprise Upgrade and remain compliant?

Options:

A- Retiring from fleet

B- Different model replacement

C- ChromeOS Flex upgrade transfer

D- Same model replacement

Answer:

B

Explanation:

When deprovisioning ChromeOS devices for a hardware recall and replacement with different models, choosing the 'Different model replacement' option is crucial to retain the Chrome Education/Enterprise Upgrade license compliance. This option ensures that the license is transferred to the new device correctly, avoiding any compliance issues or the need to repurchase licenses.

Here's why this option is important:

License Transfer:It specifically designates the deprovisioning as being due to a hardware replacement with a different model.This triggers the system to transfer the license to the new device upon enrollment.

Compliance:It maintains the compliance of your Chrome Education/Enterprise Upgrade licenses,ensuring you don't violate any licensing terms.

Cost Savings:It avoids the need to purchase new licenses for the replacement devices,saving your organization money.

Question 10

Question Type: **MultipleChoice**

A user reports that their Chrome device has been stolen. What should the administrator do?

Options:

A- Use the Google Admin console to turn on the stolen Chromebook's webcam

B- Use the Google Android Device Manager to locate the Chromebook

C- Set the stolen Chromebook lo disabled mode to prevent user sign-ins

D- Remotely wipe user data from the Chromebook

Answer:

C

Explanation:

When a Chrome device is reported stolen, the administrator should immediately take action to protect the data and prevent unauthorized access. The most effective step is to disable the device through the Google Admin console. This will prevent anyone from signing in to the device, rendering it unusable.

Here's how to disable a stolen Chrome device:

Sign in to Google Admin console:Use your administrator credentials.

Navigate to Devices:Go to Devices > Chrome > Devices.

Locate the Device:Find the stolen device using its serial number or other identifying information.

Disable the Device:Click on the device and select 'Disable.'

This will disable the device and prevent anyone from signing in, even if they try to reset the device.

Question 11

Question Type: MultipleChoice

What is needed for an admin to remote desktop to a user or managed guest session devices with the Admin console?

Options:

A- The user must accept the connection request

B- The user must share the session pin with the admin

C- Both the admin and the remote device must be on the same network

D- The admin must be in the same OU as the remote device

Answer:

A

Explanation:

To initiate a remote desktop session to a ChromeOS device using the Admin console, the administrator needs the user's consent. The remote desktop feature works by sending a connection request to the user's device, which they must explicitly accept before the session can start. This ensures user privacy and prevents unauthorized access.

Question 12

Question Type: MultipleChoice

An admin is setting up third-party SSO for their organization as the super admin. When they test with their account, they do not see the SSO screen.

What is causing this behavior?

Options:

A- SSO settings are misconfigured

B- The account is in the wrong OrgUnit

C- Third-party SSO is not enabled

D- Super admin bypassed the thud-patty

Answer:

D

Explanation:

Super administrators in Google Workspace have special privileges that allow them to bypass certain security features, including third-party SSO. This is to ensure that they can always access the Admin console for troubleshooting or critical changes, even if the SSO system is malfunctioning. Therefore, when a super admin tests third-party SSO, they won't be prompted with the SSO login screen, but will directly access the console using their Google credentials.