Google

Exam Questions ChromeOS-Administrator

Professional ChromeOS Administrator Exam

NEW QUESTION 1
A customer deploys a large number of ChromeOS devices and would like to start the process of turning on Zero-Touch Enrollment (ZTE) to streamline their deployment process. As an administrator, what would be required to enable ZTE?

A. Identify OU to place devices during enrollment
B. Grant partner admin access
C. Create a pre-provisioning token
D. Create a zero-touch token

Answer: C

Explanation:
To enableZero-Touch Enrollment (ZTE)for ChromeOS devices, an administrator must firstcreate a pre-provisioning token. This token allows devices to automatically enroll when they are first powered on and connected to the internet. The pre-provisioning token links the device to the correct organization and management policies.
Verified Answer from Official Source:
The correct answer is verified from theGoogle Zero-Touch Enrollment Guide, which outlines the process of setting up pre-provisioning tokens for automated enrollment.
"To set up Zero-Touch Enrollment, generate a pre-provisioning token in the Admin console and configure it with the device provider."
Creating the token ensures that new devices are automatically configured and enrolled without manual intervention, saving time during mass deployments.
Objectives:
? Automate ChromeOS device enrollment.
? Simplify large-scale deployments.
References:
Google Zero-Touch Enrollment Guide

NEW QUESTION 2
Which management feature makes ChromeOS devices a popular choice for IT administrators in educational organizations and enterprises?

A. Inability to remotely control and monitor devices
B. Centralized management through Admin console
C. Remote BIOS controls and firmware update
D. Secure management through on-prem infrastructure

Answer: B

Explanation:
ChromeOS devices are favored in educational and enterprise settings due to their centralized management via the Google Admin console. This tool allows IT administrators to manage thousands of devices from a single interface, applying policies, updates, and monitoring remotely.
Verified Answer from Official Source:
The correct answer is verified from theChromeOS Enterprise Management Guide, which emphasizes the use of the Admin console for device and user management.
"The Admin console provides a centralized platform to manage ChromeOS devices, including policy application, device monitoring, and updates."
This feature streamlines management tasks, saving time and ensuring consistent policy enforcement across an organization.
Objectives:
? Efficient device management in enterprise environments.
? Utilize the Admin console for centralized control.
References:
ChromeOS Enterprise Management Guide

NEW QUESTION 3
Your security department wants to mitigate the risk of data loss in the case of stolen equipment. As a ChromeOS Administrator, you want to ensure that your ChromeOS devices will be able to stay enterprise-managed. What should you do?

A. Add a disabled device return instruction message.
B. Enable the Autocomplete domain feature.
C. Force devices to automatically re-enroll after wiping.
D. Allow users into your organization to enroll new or re-enroll existing devices.

Answer: C

Explanation:
Enabling Forced Re-enrollment ensures that even if a device is wiped (Powerwashed), it will automatically re-enroll into the management domain once it connects to the internet. This feature is crucial for maintaining control and management over devices, particularly in cases of theft or loss.
Verified Answer from Official Source:
The correct answer is verified from theGoogle ChromeOS Management Best Practices, where it states that forced re-enrollment helps maintain device management post-wipe.
"When forced re-enrollment is enabled, devices that are wiped are automatically re- enrolled into your domain when connected to the internet."
This setting ensures that the device will always be managed by the organization, regardless of whether it has been wiped, thus mitigating data loss risks.
Objectives:
? Manage device security and data integrity.
? Implement forced re-enrollment for ChromeOS devices.
References:
ChromeOS Management Best Practices

NEW QUESTION 4
Your organization is using a third-party IdP. Users report that they can only log in to the device when connected to the Internet. Which setting is causing this problem?

A. Online revocation checks
B. Single sign-on cookie behavior
C. SAML single sign-on login frequency
D. Single sign-on IdP redirection

Answer: C

Explanation:
When using athird-party Identity Provider (IdP)with SAML-based Single Sign-On (SSO), users might only be able to log in when connected to the Internet if theSAML single sign-
on login frequencysetting is configured in a way that requires online authentication. This configuration means that users must reauthenticate against the IdP whenever they log in, rather than using cached credentials.
Verified Answer from Official Source:
The correct answer is verified from theGoogle ChromeOS SSO Configuration Guide, which specifies that configuring login frequency to "Always" forces online reauthentication.
"If the SAML single sign-on login frequency is set to 'Always', users must be online to authenticate through the third-party IdP each time they log in."
To allow offline login, configure the setting to allow cached credentials, which enables users to log in even without an active Internet connection.
Objectives:
? Enable offline login for SAML-based SSO.
? Manage login frequency settings effectively.
References:
Google ChromeOS SSO Configuration Guide

NEW QUESTION 5
To use Verified Access in your organization, you need to have a Chrome extension that calls Verified Access API on the client devices. Where can you go to get this extension?

A. Google Play Store
B. Independent software vendor (ISV) or Google Verified Access API
C. Independent software vendor (ISV) repository
D. Software API Key store

Answer: B

Explanation:
Verified Access requires a Chrome extension to communicate with the Verified Access API. While Google doesn't directly provide this extension, it offers detailed documentation and resources through the Verified Access API. Independent software vendors (ISVs) can use these resources to develop and provide compatible extensions. Option A is incorrectbecause Google Play Store is for Android apps, not Chrome extensions.
Option C is incorrectbecause while ISVs might offer extensions, it's not the sole source. Google's documentation is essential.
Option D is incorrectbecause API keys are for authentication, not the extension itself.

NEW QUESTION 6
All of your kiosk devices must update only during certain hours. Which setting is required?

A. Release channel
B. Blackout windows
C. Version pinning
D. Rollout plan

Answer: B

Explanation:
To restrict updates to specific time frames, configureBlackout windowsin the Admin console. Blackout windows allow administrators to specify periods during which ChromeOS devices are not allowed to update. This feature is particularly useful for kiosk devices, where unexpected updates could disrupt operations.
Verified Answer from Official Source:
The correct answer is verified from theGoogle ChromeOS Update Management Guide, which specifies that blackout windows help control update timing.
"Configure blackout windows to prevent ChromeOS devices from updating during specified hours, ensuring that kiosks remain functional during business operations."
Blackout windows are essential for environments where uptime is critical, such as retail kiosks or customer service points, as they prevent disruptions caused by automatic updates.
Objectives:
? Control update schedules for ChromeOS devices.
? Maintain device availability during operational hours.
References:
Google ChromeOS Update Management Guide

NEW QUESTION 7
What is a best practice for admin accounts on the Google Admin console?

A. Super Admins should be used for all changes to the domain
B. Group Admins should have 2FA enabled only if given security policy controls
C. Super Admins should use a separate user account tor day-to-day activities
D. Group Admins should have access to multiple groups

Answer: C

Explanation:
The principle of least privilege dictates that users should only have the minimum access necessary to perform their job functions. This applies to super admins as well. Using a separate user account for daily activities reduces the risk of accidental misconfiguration or unauthorized changes due to the elevated privileges associated with the super admin role.

? Security: By using a separate account, super admins limit the potential attack
surface in case their regular account is compromised.
? Accountability: It's easier to track actions and changes when different accounts are used for different purposes.
? Recovery: If the super admin account is locked or disabled, having a separate account allows for easier recovery.

NEW QUESTION 8
You want to restrict who can sign in to a managed device during working hours. Which two settings do you need to use?
Choose 2 answers

A. Single sign-on IdP redirection
B. Device oft hours
C. User Data (Ephemera))
D. Family Link accounts

Answer: BD

Explanation:
? Device off hours: This setting allows you to specify times when the device cannot be used, effectively restricting access to certain hours.
? Family Link accounts: Family Link is a parental control app that allows you to manage a child's account and device usage. By requiring Family Link accounts, you can enforce sign-in restrictions for younger users.
Other options are incorrect because:
? A: Single sign-on (SSO) redirection simplifies sign-in for authorized users, but doesn't inherently restrict access.
? C: User Data (Ephemeral) controls whether user data is saved locally, but doesn't restrict sign-in.
References: https://support.google.com/chrome/a/answer/3523633 https://families.google.com/familylink/

NEW QUESTION 9
What are two ways customers can open a support case for ChromeOS? Choose 2 answers

A. Chat support via the Admin console
B. Contact the device manufacturer
C. File feedback on the device with Alt + Shift +1
D. File case through Customer Care Portal
E. Send an email to ChromeOS support

Answer: BD

Explanation:
? B. Contact the device manufacturer: ChromeOS devices are manufactured by
various companies like Acer, HP, Lenovo, etc. Each manufacturer provides its own support channels, including phone, email, or chat support. Customers can contact the manufacturer for hardware-related issues or specific device configurations.
? D. File a case through the Customer Care Portal: Google provides a customer
care portal where customers can submit support cases online. This portal allows users to describe their issues, attach relevant files, and track the progress of their case.
Why other options are incorrect:
? A. Chat support via the Admin console: Chat support is usually available for enterprise customers with Chrome Enterprise Upgrade or Google Workspace, not individual ChromeOS users.
? C. File feedback on the device with Alt + Shift + 1: This keyboard shortcut is used to capture screenshots and send feedback to Google, but it doesn't directly open a support case.
? E. Send an email to ChromeOS support: While Google has support
channels, sending a general email might not be the most efficient way to open a case and get a timely response.
References:
Get support - Chrome Enterprise and Education Help:
https://support.google.com/chrome/a/answer/4594885?hl=en

NEW QUESTION 10
You want users to sign in to ChromeOS devices via SAML Single Sign-On and be able to access websites and cloud services that rely on the same identity provider without having to re-enter credentials. How should you configure SAML?

A. Enable SAML identity provider-initialed login for Google authentication
B. Enable SAML-based Single Sign-On for ChromeOS devices and set the Single Sign-On cookie behavior to enable transfer of SAML SSO cookies into user sessions during login
C. Enable SAML-based Single Sign-On for each application via Chrome App Management
D. Use Chrome App Builder to enable SSO for application and force-install the application using ChromeOS user policies

Answer: B

Explanation:
To achieve seamless SSO between ChromeOS devices and other web services using the same identity provider, you need to configure SAML SSO in the Google Admin console:
? Enable SAML-based SSO for ChromeOS devices.
? In the SSO settings, find theSingle Sign-On cookie behaviorand set it to "Enable transfer of SAML SSO cookies into user sessions during login." This allows the SAML authentication cookie to be passed between the ChromeOS login and other web services, eliminating the need for re-authentication.
Option A is incorrect because it relates to the initial login method, not cookie transfer for subsequent SSO.
Options C and D are incorrect because they involve application-specific SSO configurations, not the general SAML SSO setup for the device.

NEW QUESTION 10
You need to get to the enterprise enrollment screen. What should you do?

A. Press Ctrl-Alt-E during the Chrome bootup sequence (Chrome logo animation)

B. Sign in with enterprise enrollment credentials provided by the customer at the user sign- in screen
C. Press Ctrl-Alt-F on the initial welcome screen to set initial settings
D. Press Ctrl-Alt-E at the user login screen before any user has signed in to the device

Answer: A

Explanation:
? Power on or reboot the Chromebook.
? Watch for the Chrome logo animation.This is the key moment to trigger enterprise enrollment.
? Press Ctrl+Alt+E simultaneously.This keyboard shortcut interrupts the normal boot process and redirects the Chromebook to the enterprise enrollment screen.
? Follow the on-screen instructions.You'll be prompted to enter information such as the domain name of the organization and enrollment credentials.
Why this is the correct method:
? Enterprise Enrollment Timing:The Ctrl+Alt+E shortcut is specifically designed to be used during the bootup sequence, before any user profile is loaded. This ensures the device is enrolled in the organization's management system from the start.
? Alternative Options:The other options mentioned are incorrect:
References:
Enroll a Chrome device:https://support.google.com/chrome/a/answer/1360534?hl=en

NEW QUESTION 12
A customer is setting up a new Google tenant. You have been tasked with creating the organization unit structure for the Google Admin console. Following Google best practices, how should you set up the new organization units?

A. Recreate the same OU structure as the current LDAP implementation
B. Combine Devices and Users into single OUs to avoid operational overhead
C. Follow a hierarchical OU structure
D. Use shortest possible names for OUs to avoid confusion

Answer: C

Explanation:
Followinga hierarchical OU structureallows for clear and organized management of devices and users. This structure mirrors real-world organizational layouts (such as departments or geographical locations), which makes applying policies and managing devices more straightforward.
Verified Answer from Official Source:
The correct answer is verified from theGoogle Admin Console Best Practices Guide, which recommends using hierarchical OUs for clarity and ease of management.
"Using a hierarchical OU structure makes it easier to manage devices and users separately, especially when applying specific policies."
A well-organized OU structure improves scalability and simplifies policy management, reducing administrative complexity.
Objectives:
? Implement structured and manageable OU setups.
? Follow best practices for organizational hierarchy in Google Admin Console.
References:
Google Admin Console Best Practices Guide

NEW QUESTION 15
A customer deploys a large number of ChromeOS devices and would like to start the process of turning on Zero-Touch Enrollment (ZTE) to streamline their deployment process. As an administrator, what would be required to enable ZTE?

A. Grant partner admin access
B. identify OU to place devices during enrollment
C. Create a zero-touch token
D. Create a pre-provisioning token

Answer: B

Explanation:
Zero-touch enrollment (ZTE) automates the device enrollment process when users first power on their ChromeOS devices. Before you can enable ZTE, you need to determine the organizational unit (OU) where the devices should be placed during enrollment. This is crucial because different OUs can have different policies and configurations applied to them.
? Plan Your OU Structure: If you haven't already, create a well-organized OU
structure in your Google Admin console that reflects your organization's hierarchy and device management needs.
? Select the Target OU: Choose the specific OU where you want the ZTE-enrolled
devices to reside. Consider factors like department, location, or device type when making your decision.
Once you've identified the appropriate OU, you can proceed with creating a zero-touch enrollment token and associating it with that OU. This will ensure that newly enrolled devices are automatically placed in the correct OU and inherit the desired policies.

NEW QUESTION 19
Due to security threats, your security team would like to immediately prevent any apps on a ChromeOS device from being able to use USB devices. How can you as the admin implement this security practice as quickly and efficiently as possible?

A. Create an allowlist and add apps that do not need USB permissions
B. Create a blocklist and add apps that use USB permissions
C. Create a blocklist, add apps that use USB permissions, and allow users to 'request' apps that are not approved
D. Block apps by using the "Block apps by permissions settings" which will allow you to select "USB" as permission type to block

Answer: D

Explanation:
To quickly block apps from accessing USB devices on ChromeOS, use the"Block apps by permissions" settingsin the Admin console. Selecting"USB"as the permission type ensures that no application on the device can interact with USB peripherals, mitigating potential security threats.
Verified Answer from Official Source:

The correct answer is verified from theGoogle ChromeOS Application and Device Management Guide, which details using permission-based blocking for enhanced security.
"To block applications from using USB devices, configure the 'Block apps by permissions' setting in the Admin console and select 'USB' as the restricted permission."
This method provides a comprehensive and quick way to mitigate USB-based threats without individually managing each application.
Objectives:
? Strengthen ChromeOS device security.
? Manage app permissions effectively.
References:
Google ChromeOS Application and Device Management Guide

NEW QUESTION 24
A ChromeOS Administrator has deployed ChromeOS devices in their organization. How can the company evaluate the compatibility with future updates following Google's best practices while still gaining access to new features when they launch?

A. Enable "Auto Updates" on all devices on the 'Stable channel*, but let the employees in the IT department run their devices on the "Beta channel* so they have time to evaluate and adapt the environment to each update before it reaches Stable
B. Disable ????Auto Updates???? on all devices and let the admin test the newest release on the "Stable channel" on their own device before rolling it out organization-wide
C. Set 5% of the organization across several departments on the 'Beta channel"1, and configure the rest of the fleet to receive auto updates onthe "Stable channel'
D. Set the entire fleet to update in accordance with the "Long-term Support (LTS) channel"

Answer: A

Explanation:
This approach balances access to new features with controlled testing. Here's how it works:
? Stable Channel:Most devices receive automatic updates on the Stable channel,
ensuring security and stability for the majority of users.
? Beta Channel:IT staff use the Beta channel to access updates earlier, allowing them to identify and address potential issues before they affect the entire organization.
? Evaluation and Adaptation:IT staff can test compatibility, adjust configurations, and prepare for broader deployment based on their experience with the Beta channel.
Option B is incorrectbecause disabling auto-updates compromises security and delays access to new features.
Option C is incorrectbecause while a small beta group is useful, it might not be enough to cover all potential issues.
Option D is incorrectbecause the LTS channel focuses on stability, not early access to new features.

NEW QUESTION 25
Help Desk administrators need a limited set of privileges to perform actions in the Google Admin console. How should an administrator grant these permissions while conforming to the practice of least privilege?

A. Create a Service Desk Group and add Service Desk admins to the group
B. Create a new custom admin role and assign
C. Grant service desk administrators the Services Admin Role
D. Allow Help Desk administrators full access to manage users

Answer: B

Explanation:
? How to Create a Custom Admin Role:
Why Other Options Are Less Ideal:
? A. Service Desk Group: Groups are primarily for organization and don't provide granular permission control.
? C. Services Admin Role: This role has broader permissions than what a Help Desk typically needs, violating the PoLP.
? D. Full Access: This grants excessive privileges and significantly increases the risk of accidental or intentional misuse.

NEW QUESTION 29
How do you validate Chrome policies on a managed device?

A. Go to the admin console and look up the policies
B. Download device logs
C. In the browser, go to chrome://policy to confirm that the device is receiving both user and device policy
D. In the browser, go to policy://chrome to confirm that the device is receiving both user and device policy

Answer: C

Explanation:
To check which policies are applied to a ChromeOS device, navigate tochrome://policyin the Chrome browser. This page displays a list of all policies applied to the device, including both user-specific and device-specific policies. This is the most accurate way to verify that the device is receiving the correct policies from the Google Admin console.
Verified Answer from Official Source:
The correct answer is verified from theGoogle Chrome Enterprise Policy Guide, which recommends using thechrome://policyURL to review current policy settings on a device.
"To see the policies applied to a ChromeOS device, open Chrome and go to chrome://policy. This page lists both user and device policies that are currently enforced."
This method allows administrators to validate the application of policies directly on the device, confirming that updates from the Admin console have been successfully applied. Objectives:
? Validate policy application on managed ChromeOS devices.
? Use chrome://policy to troubleshoot policy issues.
References:
Google Chrome Enterprise Policy Guide

NEW QUESTION 31
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?

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.

NEW QUESTION 36
As an administrator, you would like the ability to see and test upcoming changes to the Google Admin console. How would an admin get access to pre-release features and upcoming ChromeOS device management changes to the Admin console?

A. Enroll in the ChromeOS Factory Software Platform
B. Join the Chrome Enterprise BETA Testing
C. Register for the Chrome Enterprise Trusted Tester Program
D. Create a ChromeQS Developer Account

Answer: C

Explanation:
The Chrome Enterprise Trusted Tester Program is designed for administrators who want early access to pre-release features and changes in the Google Admin console, including those related to ChromeOS device management. By joining this program, administrators can:
? Test New Features: Get hands-on experience with upcoming features and
changes before they are officially released.
? Provide Feedback: Share feedback directly with Google's product teams, helping to shape the development and prioritization of new functionalities.
? Stay Ahead: Be among the first to know about new capabilities and improvements in the Google Admin console.
How to Register:
? Visit the Chrome Enterprise Trusted Tester Program
website: https://inthecloud.withgoogle.com/trusted-testers/sign-up.html
? Fill out the registration form with your organization's details.
? Google will review your application and, if approved, provide you with access to pre-release features.
References:
Become a Chrome Enterprise Trusted Tester:
https://support.google.com/chrome/a/answer/9036081?hl=en

NEW QUESTION 40
Which management feature makes ChromeOS devices a popular choice for IT administrators in educational organizations and enterprises?
Which management feature makes ChromeOS devices enterprises?

A. Secure management through on prem infrastructure
B. Remote BIOS controls and firmware update
C. Centralized management through Admin console
D. Inability to remotely control and monitor devices

Answer: C

Explanation:
The ChromeOS Admin console provides centralized management, making it a popular choice for IT administrators. It allows them to manage policies, apps, extensions,
and device settings from a single interface, streamlining administration and ensuring consistency across devices.
Option A is incorrectbecause ChromeOS management is primarily cloud-based, not on- premises.
Option B is incorrectbecause while BIOS control might be available, it's not the primary management feature.
Option D is incorrectbecause ChromeOS devices can be remotely controlled and monitored through the Admin console.
References:
About ChromeOS device management:
https://support.google.com/chrome/a/answer/1289314?hl=en

NEW QUESTION 42
The finance team for an organization buys a new printer to print sensitive documents without using the main office printer. How should you automatically configure the printer for finance team users?

A. Deploy correct drivers to the finance devices
B. Deploy the printer via Groups
C. Add the printer directly to the user
D. Plug the new printer directly into the router

Answer: B

Explanation:
To configure the printer specifically for finance team users, the most efficient approach is to deploy the printer via Groups. By assigning the printer to a Google Group that contains finance team members, the printer will automatically be available to all users in that group without manual configuration for each device.
Verified Answer from Official Source:
The correct answer is verified from theGoogle Admin Console Printing Configuration Guide, which recommends using Groups to deploy printers for specific user sets.
"Deploy printers to user groups to ensure that only specified users have access. Use the Groups feature to manage printer availability efficiently."
Using Groups for printer deployment ensures that only authorized users (in this case, finance team members) can print sensitive documents, maintaining security and ease of access.
Objectives:
? Secure printer access for specific user groups.
? Simplify printer configuration for departments.
References:
Google Admin Console Printing Configuration Guide

NEW QUESTION 45
A user reports that their Chrome device has been stolen. What should the administrator do?

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.

NEW QUESTION 48
You're in charge of deploying video conferencing equipment and it has been decided that you will leverage ChromeOS devices. What initial considerations should you make when
deciding on devices?

A. Deploying instructional guides to all users on setup configuration, and use of new equipment
B. A form factor compatible for both remote and site workers is required
C. A precise time window on how to apply security patches and updates to all devices
D. Devices must have 8GB of RAM and obey supported processor models

Answer: B

Explanation:
When deploying video conferencing equipment using ChromeOS devices, the primary consideration is choosing a form factor (device type) that caters to both remote and on-site workers. This ensures flexibility and consistent user experience regardless of location.
Option A is incorrectbecause while instructional guides are helpful, they are a secondary concern to device suitability.
Option C is incorrectbecause security patch timing is important but not the initial consideration when choosing devices.
Option D is incorrectbecause while specifications matter, they should align with the chosen form factor and user needs.

NEW QUESTION 50
You have been asked to explain the built-in security features of ChromeOS. What i3 the benefit of having verified boot enabled on a ChromeOS device?

A. It ensures that the OS is uncompromised
B. It allows updates to happen in the background
C. Running both operating systems on one device at the same time makes It twice as powerful
D. It installs the known safe backup OS every time the device is slatted up.

Answer: A

Explanation:
Verified Boot in ChromeOS is a security mechanism that checks the integrity of the operating system during startup. If it detects any unauthorized modifications or compromises, it can initiaterecovery processes to restore the OS to a known good state, ensuring that the device boots up with a secure and untampered operating system. Option B is incorrectbecause background updates are a separate feature.
Option C is incorrectbecause dual-boot is not related to Verified Boot.
Option D is incorrectbecause Verified Boot doesn't install a backup OS but verifies the existing one.
Verified Boot:https://www.chromium.org/chromium-os/chromiumos-design-docs/verified- boot/

NEW QUESTION 53
You need to create a recovery image on a USB stick. Which two steps should you take? Choose 2 answers

A. Go to Device Settings
B. Go lo google com/chromebooks

C. Go to Google Play store
D. Go to Chrome Web Store on a Chrome device
E. Install Chrome Recovery Utility and download the image for the coned device model to a USB stick

Answer: DE

Explanation:
To create a recovery image on a USB stick, you need to:
? Access Chrome Web Store: Open the Chrome Web Store on a Chrome device (either a Chromebook or a computer with the Chrome browser installed).
? Install Chromebook Recovery Utility: Search for and install the "Chromebook Recovery Utility" extension.
? Launch the Utility: Open the installed extension.
? Identify Device: Enter the model number of the ChromeOS device for which you want to create the recovery image.
? Insert USB Stick: Insert a USB stick with sufficient storage capacity (at least 4GB).
? Download and Create: Follow the on-screen instructions in the utility to download the correct recovery image and create the bootable USB stick.
This process will prepare a USB stick that can be used to recover or reinstall ChromeOS on a device that is not functioning properly.
References:
Recover your Chromebook:
https://support.google.com/chromebook/answer/1080595?hl=en

NEW QUESTION 58
Your organization's security protocols require you to ensure that any unattended devices log the user out after 24 hours. You have 1000 ChromeOS devices to manage. How would you Implement this with the least amount of admin effort?

A. Enable the 'User and Browser Settings" and update 'Maximum user session length* to any time up to 24 hours
B. Create a corporate policy stating (he users are to manually sign out after the end of every shift
C. You can remotely access each device and sign out of the user account using Chrome Remote Desktop
D. Force-install a custom app to each device in question that notifies the user that they need to sign out of their device after 24 hours

Answer: A

Explanation:
This is the most efficient method as it applies the setting to all devices within the organizational unit (OU) through a single policy change in the Admin console.
The other options are less efficient:
? Corporate policy:Relies on user compliance and is difficult to enforce.
? Chrome Remote Desktop:Requires manual intervention for each device.
? Custom app:Adds complexity and potential security risks.
References:
Set up Chrome browser on managed devices:
https://support.google.com/chrome/a/answer/3523633?hl=en

NEW QUESTION 60
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

ChromeOS-Administrator Practice Exam Features:

* ChromeOS-Administrator Questions and Answers Updated Frequently

* ChromeOS-Administrator Practice Questions Verified by Expert Senior Certified Staff

* ChromeOS-Administrator Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* ChromeOS-Administrator Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year