

100% Associate-Google-Workspace-Administrator Correct Answers & Real Associate-Google-Workspace-Administrator Dumps

Google Workspace Admin Certification Exam

Your company is using Google Workspace Enterprise Standard. They have 200 meeting rooms defined for the main building and used daily by the 12,000 employees. Users are complaining they have difficulties finding a room available when searching within Google Calendar, even if several rooms are available (no one attending meetings in these rooms at that time). You have been asked to find a solution while minimizing the operational effort and avoiding any new expenses due to budget constraints. What should you do?

- A. Implement a third-party solution that will detect presence in the room and release it if nobody appears after a few minutes.
- B. Create a Google App Script that will inspect each room calendar for the next 12 hours, check attendees status, and send the room administrator an alert email for releasing the room if all attendees have declined but the room has not.
- C. Set the option "Allow calendar-based room release" for all targeted rooms. - Answer C. Set the option "Allow calendar-based room release" for all targeted rooms.

Your company has just acquired a new group of users. They have been provisioned into the Google Workspace environment with your primary domain as their primary email address. These new users still need to receive emails from their previous domain. What is the best way to achieve this for these new users, without updating the information of preexisting users?

- A. Add the acquired domain as an alias to the primary Google Workspace domain.
- B. Add the acquired domain as a secondary domain to the primary Google Workspace domain, and then update the email information of all new users with alias emails.
- C. Update the Google-provided test domain to be the domain of the acquired company, and then update the email information of all new users with alias emails.
- D. Without adding a domain, update each user's email information with the previous domain. - Answer A. Add the acquired domain as an alias to the primary Google Workspace domain.

The application development team requests that a new, internal, domain-owned Google Workspace app be allowed to access Google Drive APIs. You are currently restricting access to all APIs using an approved allowlist, per security policy. You need to grant access for this app. What should you do?

What's more, part of that PrepAwayExam Associate-Google-Workspace-Administrator dumps now are free:

https://drive.google.com/open?id=12kPnFYRxA3Dte_-FxnA7fEQuTRcupBZG

PrepAwayExam addresses this issue by offering real Google Associate-Google-Workspace-Administrator Questions. PrepAwayExam's team of professionals worked tirelessly to create the Associate-Google-Workspace-Administrator questions, ensuring that applicants have access to the most recent and genuine Associate-Google-Workspace-Administrator Exam Questions. With PrepAwayExam's help, you can pass the Associate-Google-Workspace-Administrator exam on your first attempt or claim a refund according to certain terms and conditions.

Google Associate-Google-Workspace-Administrator Exam Syllabus Topics:

| Topic | Details |
|-------|---------|
| | |

| | |
|---------|--|
| Topic 1 | <ul style="list-style-type: none"> • Data Access and Authentication: This section of the exam evaluates the capabilities of Security Administrators and focuses on configuring policies that secure organizational data across devices and applications. It includes setting up Chrome and Windows device management, implementing context-aware access, and enabling endpoint verification. The section assesses the ability to configure Gmail Data Loss Prevention (DLP) and Access Control Lists (ACLs) to prevent data leaks and enforce governance policies. Candidates must demonstrate an understanding of configuring secure collaboration settings on Drive, managing client-side encryption, and restricting external sharing. It also covers managing third-party applications by controlling permissions, approving Marketplace add-ons, and deploying apps securely within organizational units. Lastly, this section measures the ability to configure user authentication methods, such as two-step verification, SSO integration, and session controls, ensuring alignment with corporate security standards and compliance requirements. |
| Topic 2 | <ul style="list-style-type: none"> • Configuring Services: This section of the exam evaluates the expertise of IT Systems Engineers and emphasizes configuring Google Workspace services according to corporate policies. It involves assigning permissions, setting up organizational units (OUs), managing application and security settings, and delegating Identity and Access Management (IAM) roles. The section also covers creating data compliance rules, applying Drive labels for data organization, and setting up feature releases such as Rapid or Scheduled Release. Candidates must demonstrate knowledge of security configurations for Google Cloud Marketplace applications and implement content compliance and security integration protocols. Furthermore, it includes configuring Gmail settings such as routing, spam control, email delegation, and archiving to ensure communication security and policy alignment across the organization. |
| Topic 3 | <ul style="list-style-type: none"> • Troubleshooting: This section of the exam measures the skills of Technical Support Specialists and focuses on identifying, diagnosing, and resolving issues within Google Workspace services. It tests the ability to troubleshoot mail delivery problems, interpret message headers, analyze audit logs, and determine root causes of communication failures. Candidates are expected to collect relevant logs and documentation for support escalation and identify known issues. The section also evaluates knowledge in detecting and mitigating basic email attacks such as phishing, spam, or spoofing, using Gmail security settings and compliance tools. Additionally, it assesses troubleshooting skills for Google Workspace access, performance, and authentication issues across different devices and applications, including Google Meet and Jamboard, while maintaining service continuity and network reliability. |
| Topic 4 | <ul style="list-style-type: none"> • Supporting Business Initiatives: This section of the exam measures the skills of Enterprise Data Managers and covers the use of Google Workspace tools to support legal, reporting, and data management initiatives. It assesses the ability to configure Google Vault for retention rules, legal holds, and audits, ensuring compliance with legal and organizational data policies. The section also involves generating and interpreting user adoption and usage reports, analyzing alerts, monitoring service outages, and using BigQuery to derive actionable insights from activity logs. Furthermore, candidates are evaluated on their proficiency in supporting data import and export tasks, including onboarding and offboarding processes, migrating Gmail data, and exporting Google Workspace content to other platforms. |
| Topic 5 | <ul style="list-style-type: none"> • Managing Objects: This section of the exam measures the skills of Google Workspace Administrators and covers the management of user accounts, shared drives, calendars, and groups within an organization. It assesses the ability to handle account lifecycles through provisioning and deprovisioning processes, transferring ownership, managing roles, and applying security measures when access needs to be revoked. Candidates must understand how to configure Google Cloud Directory Sync (GCDS) for synchronizing user data, perform audits, and interpret logs. Additionally, it tests knowledge of managing Google Drive permissions, lifecycle management of shared drives, and implementing security best practices. The section also focuses on configuring and troubleshooting Google Calendar and Groups for Business, ensuring proper access control, resource management, and the automation of group-related tasks using APIs and Apps Script. |

>>> 100% Associate-Google-Workspace-Administrator Correct Answers <<<

**Pass Guaranteed Google - Associate-Google-Workspace-Administrator
Accurate 100% Correct Answers**

Many candidates find the Google exam preparation difficult. They often buy expensive study courses to start their Google Associate-Google-Workspace-Administrator certification exam preparation. However, spending a huge amount on such resources is difficult for many Associate Google Workspace Administrator applicants. The Latest Associate-Google-Workspace-Administrator Exam Dumps are the right option for you to prepare for the Associate-Google-Workspace-Administrator certification test at home.

Google Associate Google Workspace Administrator Sample Questions (Q22-Q27):

NEW QUESTION # 22

Your organization allows employees to use their personal mobile devices to check their work emails. You need to remove the employee's work email data from their phone when they leave the organization. What should you do?

- A. Set up 2SV authentication on the devices.
- B. Set up basic mobile management on the devices.
- C. Set up data protection rules to prevent data sharing externally.
- **D. Set up advanced mobile management on the devices.**

Answer: D

Explanation:

With advanced mobile management, you can remotely manage and wipe work-related data from personal devices when an employee leaves the organization. This includes the ability to enforce policies such as requiring a password to access the device, remotely wiping corporate data, and managing access to work resources without affecting the personal data on the device. This solution provides the necessary tools to ensure data security and compliance.

NEW QUESTION # 23

Your organization is increasingly concerned about its environmental impact. You want to assess the environmental impact of using Google Workspace services. Which report should you use?

- **A. Carbon footprint report**
- B. Google Environmental Report
- C. Apps Monthly Uptime report
- D. Accounts report

Answer: A

Explanation:

To assess the environmental impact of using Google Workspace services, you should refer to the Google Environmental Report. Google publishes comprehensive reports detailing its environmental efforts, including the energy efficiency of its data centers, its use of renewable energy, and its overall carbon footprint, which includes the impact of services like Google Workspace.

Here's why option B is the correct choice and why the others are not relevant to assessing the overall environmental impact of using Google Workspace:

B . Google Environmental Report

Google regularly publishes detailed environmental reports that cover various aspects of its sustainability initiatives, including its progress towards using renewable energy, its efforts to improve energy efficiency in its operations (which power Google Workspace), and its overall carbon footprint. These reports provide insights into the environmental impact associated with using Google services.

Associate Google Workspace Administrator topics guides or documents reference: While there might not be a specific "Google Workspace Environmental Impact Report" as a standalone document within the Admin console, Google's overarching "Environmental Report" (often found on Google's sustainability or environmental responsibility websites) encompasses the infrastructure and practices that support all Google services, including Google Workspace. Administrators looking for this information would be directed to these publicly available Google reports.

A . Carbon footprint report

While the concept of a "carbon footprint report" is relevant to environmental impact, Google typically includes this information within its broader "Environmental Report" rather than providing a separate report specifically for Google Workspace usage within an organization's Admin console. You would likely find data related to the carbon efficiency of Google's infrastructure in their main environmental disclosures.

Associate Google Workspace Administrator topics guides or documents reference: Google's communication about its carbon footprint and environmental efforts is usually consolidated in their public sustainability reports.

C . Apps Monthly Uptime report

The Apps Monthly Uptime report provides information about the reliability and availability of Google Workspace services. It focuses on service performance and uptime metrics, not on environmental impact or sustainability.

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin Help documentation on service-level agreements (SLAs) and service status provides information about uptime guarantees and how to monitor service availability, which is the focus of the Apps Monthly Uptime report.

D . Accounts report

The Accounts report in the Google Admin console provides details about user accounts within your organization, such as the number of active users, account status, and other user-related information. It does not contain any data or analysis related to the environmental impact of using Google Workspace services.

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin Help documentation on reporting and user accounts describes the information available in the Accounts report, which is focused on user management and activity metrics.

Therefore, to assess the environmental impact of using Google Workspace services, your organization should refer to the publicly available Google Environmental Report, which details Google's sustainability efforts and overall environmental performance.

NEW QUESTION # 24

Your company distributes an internal newsletter that contains sensitive information to all employees by email. You've noticed unauthorized forwarding of this newsletter to external addresses, potentially leading to data leaks. To prevent this, you need to implement a solution that automatically detects and blocks such forwarding while allowing legitimate internal sharing. What should you do?

- A. Create a Gmail content compliance rule that targets the internal newsletter, identifying instances of external forwarding. Configure the rule to reject the message when such forwarding is detected
- B. Develop an Apps Script project by using the Gmail API to scan sent emails for the newsletter content and external recipients. Automatically revoke access for violating users.
- C. Add a banner to the newsletter that warns users that external sharing is prohibited.
- D. Create a content compliance rule to modify the newsletter subject line, adding a warning against external forwarding.

Answer: A

Explanation:

A Gmail content compliance rule allows you to specifically target the internal newsletter and automatically detect when it is forwarded to external addresses. By rejecting such messages, you can prevent unauthorized sharing of sensitive information while still permitting internal sharing. This solution is effective for enforcing data security policies without manual intervention.

NEW QUESTION # 25

Your company has a globally distributed remote work team. You want to ensure all team members adhere to the company's data security policies and only access authorized systems based on their location and role. What should you do?

- A. Create and enforce data loss prevention (DLP) rules to control data sharing.
- B. Set up and mandate the use of a company-wide VPN for all remote access.
- C. Implement two-factor authentication for all remote team members.
- D. Configure access control policies with conditional access.

Answer: D

Explanation:

To ensure that a globally distributed remote work team adheres to data security policies and only accesses authorized systems based on their location and role, you should configure access control policies with conditional access. Conditional access allows you to define rules that grant or block access to resources based on various factors, including the user's location, the device they are using, their role, and the application they are trying to access.

Here's why option D is the most comprehensive solution for the stated requirements and why the others address only parts of the problem:

D . Configure access control policies with conditional access.

Conditional access is a security framework that evaluates multiple signals before granting access to resources. By implementing conditional access policies, you can:

- Control access based on location: Restrict access to certain systems or data based on the geographic location of the user.

- Control access based on role: Ensure that only users with specific roles have access to certain applications or data.

- Enforce device compliance: Require users to access resources only from company-managed or compliant devices.

Implement multi-factor authentication (MFA): Require additional verification steps based on the context of the access attempt. Conditional access provides a granular and dynamic way to enforce security policies based on the specific context of each access request, aligning with the goal of allowing access only to authorized systems based on location and role while maintaining data security.

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin Help documentation on "Context-Aware Access" (which is Google's implementation of conditional access) explains how to set up policies based on user attributes (like group membership/role), device security status, and network location. This documentation details how to create access levels and assign them to applications based on specific conditions, ensuring that access is granted only when the requirements are met.

A . Create and enforce data loss prevention (DLP) rules to control data sharing.

DLP rules are crucial for preventing sensitive data from being shared inappropriately. However, they primarily focus on controlling what users can do with data after they have gained access. DLP does not, by itself, control who can access which systems based on their location and role. It's a complementary security layer but not the primary solution for access control based on these factors.

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin Help documentation on Data Loss Prevention (DLP) explains how to create rules to prevent the sharing of sensitive information. It focuses on the content of the data and user actions related to sharing, not on controlling initial access based on location and role.

B . Set up and mandate the use of a company-wide VPN for all remote access.

A VPN (Virtual Private Network) can secure the connection between remote users and the company network by encrypting traffic and potentially routing it through company-controlled servers. While it can enhance security and provide a consistent network origin, it does not inherently control access based on the user's role or their geographic location (unless the VPN infrastructure is configured to enforce such restrictions, which would be part of a broader access control strategy). Mandating a VPN is a good security practice but doesn't fully address the need for role-based and location-aware access control.

Associate Google Workspace Administrator topics guides or documents reference: Documentation on VPNs and remote access might be mentioned in the context of securing connections, but it's not the primary mechanism for implementing granular access control based on user attributes and location within Google Workspace's administrative framework.

C . Implement two-factor authentication for all remote team members.

Two-factor authentication (2FA) adds an extra layer of security by requiring users to provide two forms of identification before gaining access. This significantly reduces the risk of unauthorized access due to compromised passwords. While 2FA is a critical security measure for remote teams, it doesn't, by itself, control which systems users can access based on their location and role. It verifies the user's identity but not the context of their access attempt in terms of location or role-based authorization.

Associate Google Workspace Administrator topics guides or documents reference: The Google Workspace Admin Help strongly recommends enabling 2-Step Verification (Google's implementation of 2FA) for enhanced security. However, it is primarily focused on user authentication, not on contextual access control based on location and role.

Therefore, the most comprehensive solution to ensure adherence to data security policies and control access based on location and role for a globally distributed remote work team is to configure access control policies with conditional access. This framework allows for the creation of context-aware rules that take into account various factors to determine whether to grant or block access to resources.

NEW QUESTION # 26

Your company's security team should be able to investigate unauthorized external file sharing. You need to ensure that the security team can use the security investigation tool and you must follow the principle of least privilege. What should you do?

- A. Share the Drive audit log with the security team.
- B. Grant the super admin role to a delegate from the security team.
- **C. Create a custom admin role with security center privileges. Assign the role to the individual security team members.**
- D. Create a pre-built reporting role. Assign the role to the security team alias.

Answer: C

Explanation:

By creating a custom admin role with security center privileges, you can ensure that the security team has the necessary access to investigate unauthorized external file sharing while adhering to the principle of least privilege. This approach provides the security team with the specific permissions they need without granting unnecessary broader privileges, such as those associated with the super admin role.

NEW QUESTION # 27

.....

All of these advantages, you can avail of after passing the Associate-Google-Workspace-Administrator exam. You must find the best resource to prepare for the Google Associate-Google-Workspace-Administrator test if you want to pass the Google Associate-Google-Workspace-Administrator Certification Exam. Without proper Google Associate-Google-Workspace-Administrator exam preparation, getting success in the Google Associate-Google-Workspace-Administrator exam is impossible.

- [illegible]