Question #1 *Topic 1*

As the Workspace Administrator, you have been asked to configure Google Cloud Directory Sync (GCDS) in order to manage Google Group memberships from an internal LDAP server. However, multiple Google Groups must have their memberships managed manually. When you run the GCDS sync, you notice that these manually managed groups are being deleted. What should you do to prevent these groups from being deleted?

A. In the GCDS configuration manager, update the group deletion policy setting to “don't delete Google groups not found in LDAP.”

B. Use the Directory API to check and update the group’s membership after the GCDS sync is completed.

C. Confirm that the base DN for the group email address attribute matches the base DN for the user email address attribute.

D. In the user attribute settings of the GCDS configuration manager options, set the Google domain users deletion/suspension policy to “delete only active Google domain users not found in LDAP.”

Suggested Answer: *A*

Community vote distribution

A (100%)

RealdumpsCollection_Com Highly Voted 1 month, 3 weeks ago

Selected Answer: A

Correct A;

Users must update members manually, so exclude from the sync GCDS.

upvoted 6 times

jitu028 Highly Voted 1 year, 9 months ago

Selected Answer: A

Answer is A

https://support.google.com/a/answer/6258071?hl=en#zippy=%2Cgoogle-group-deletion-policy

Don’t delete Google Groups not found in LDAP If checked, Google Group deletions in your Google domain are disabled, even when the Groups aren't in your LDAP server.

upvoted 5 times

e6c0e9c Most Recent 1 month, 4 weeks ago

This is still valid.

upvoted 1 times

AGHPE 3 months, 1 week ago

I recommend investing in access as a collaborator. I found 80% of the questions here on the exam. You just have to pay attention to the answers but yes, they are valid!!! Thanks Examtopics

upvoted 2 times

Kim1997 3 months, 3 weeks ago

Selected Answer: A

A is correct for this.

upvoted 1 times

yuuryou 5 months ago

Are these questions still valid? Did anyone cleared the exam using this dump?

upvoted 1 times

AGHPE 4 months, 2 weeks ago

I've a same question!!

upvoted 1 times

certpavn 6 months, 4 weeks ago

I just took the exam yesterday, and there are only about 10 questions here that overlap with the questions on the exam (50).

upvoted 2 times

virat_kohli 10 months, 1 week ago

Selected Answer: A

A. In the GCDS configuration manager, update the group deletion policy setting to “don't delete Google groups not found in LDAP.”

upvoted 1 times

amministrazione 11 months, 3 weeks ago

A. In the GCDS configuration manager, update the group deletion policy setting to “don't delete Google groups not found in LDAP.”

upvoted 1 times

John_AM 1 year, 2 months ago

Took the exam today, got 19 questions from this dump

upvoted 1 times

jakeke 1 year, 2 months ago

These questions are so horribly worded and answers are so difficult. I can ace any lab or practical scenario but i feel like this exam is not going to go well at alll

upvoted 1 times

n_i_n_a 1 year, 3 months ago

Selected Answer: A

Correct A;

Users must update members manually, so exclude from the sync GCDS.

upvoted 1 times

jakeke 1 year, 2 months ago

Did you happen to take the exam? how many questions were on there? if not any, were they similar

upvoted 1 times

[Removed] 1 year, 4 months ago

Dump is not valid anymore, only a few questions in the exam and few topics not covered here...

upvoted 2 times

Debbz 1 year, 5 months ago

Selected Answer: A

In the GCDS configuration manager, update the group deletion policy setting to “don't delete Google groups not found in LDAP.

upvoted 2 times

userX100 1 year, 5 months ago

Selected Answer: A

A. In the GCDS configuration manager, update the group deletion policy setting to “don't delete Google groups not found in LDAP.

upvoted 1 times

Jameshaha 1 year, 8 months ago

Anyone passed the exam can validate the question here ?

upvoted 1 times

Tiz_Branda 1 year, 8 months ago

Hi guys, I took the exam on January 12th, I passed it but out of 50 questions only a dozen were among them. In any case, I found this forum very useful for understanding the methods of asking questions, so I recommend it but as indicated above, the questions could change

upvoted 3 times

humhead 1 year, 4 months ago

Like Tiz said, I passed the exam on April 21. But few, maybe 6 or 7 of the questions here, was on the test. But the topics here was what was used.

upvoted 1 times

jaxclain 1 year, 9 months ago

Selected Answer: A

Only correct Answer is A :)

upvoted 3 times

Question #2 *Topic 1*

Your marketing department needs an easy way for users to share items more appropriately. They want to easily link-share Drive files within the marketing department, without sharing them with your entire company. What should you do to fulfil this request? (Choose two.)

A. Create a shared drive that's shared internally organization-wide.

B. Update Drive sharing for the marketing department to restrict to internal.

C. Create a shared drive for internal marketing use.

D. Update the link sharing default to the marketing team when creating a document.

E. In the admin panel Drive settings, create a target audience that has all of marketing as members.

Suggested Answer: *BE*

Community vote distribution

CE (75%) BE (17%) 8%

impearl Highly Voted 1 year, 9 months ago

Selected Answer: CE

Check, https://support.google.com/a/answer/9934697?hl=en

upvoted 7 times

jonyuka Most Recent 3 weeks, 2 days ago

Selected Answer: CE

C. Create a shared drive for internal marketing use.

E. In the admin panel Drive settings, create a target audience that has all of marketing as members.

upvoted 1 times

virat_kohli 10 months, 1 week ago

Selected Answer: CE

C. Create a shared drive for internal marketing use.

E. In the admin panel Drive settings, create a target audience that has all of marketing as members.

upvoted 1 times

EC_Metranet 10 months, 3 weeks ago

Selected Answer: CE

You have to create the shared drive first before you update the sharing settings

upvoted 1 times

amministrazione 11 months, 3 weeks ago

C. Create a shared drive for internal marketing use.

E. In the admin panel Drive settings, create a target audience that has all of marketing as members.

upvoted 1 times

Gomesallef 12 months ago

Selected Answer: CE

Criar e mudar o publico alvo.

upvoted 1 times

BearPop 1 year, 1 month ago

CE - Definately target audiences due to link share

upvoted 1 times

jdosh 1 year, 3 months ago

Selected Answer: BE

B, because the shared drive is already created based on the question so it makes sense you restrict that to internal to avoid accidentally sharing files outside the company. E, because you want Google to tell the marketing audience automatically who are their target users for sharing so they don't get confused and share the files with other users.

upvoted 4 times

Sarilu31 1 year, 3 months ago
Notice how the keyword is "link-share", they want to link share and so "Shared Drives" is no longer in the equation (Even though it seems the most appropriate). For me it would be D and E
upvoted 2 times

Debbz 1 year, 5 months ago
Selected Answer: CE
Because a target audience is important
upvoted 3 times

userX100 1 year, 5 months ago
Selected Answer: CE
C and E
upvoted 3 times

jaxclain 1 year, 8 months ago
Selected Answer: CE
I correct myself, the correct answer is C and E because you will need a target audience to limit the marketing department not to share documents to other users internally. https://support.google.com/a/answer/10356781?fl=1#zippy=%2Climit-link-sharing-to-only-employees
upvoted 1 times

hazelcert 1 year, 9 months ago
I think DE should be correct
upvoted 1 times

jaxclain 1 year, 9 months ago
Selected Answer: BC
I also believe B and C are correct, those are the only 2 that makes sense, A and D are totally wrong... E also makes no sense if we are using Shared Drives which is Google Recommended Practices for colaboration Internally. Of course you will need a license that includes Shared Drives (Business Standard, Plus and any Enterprise.)
upvoted 2 times

RAZKZ 1 year, 9 months ago
I don't fully understand why E is incorrect in your opinion, can you rephrase please?
upvoted 1 times

jaxclain 1 year, 9 months ago
Because is a Google Best recommended practice to use Shared Drive if you want to: "They want to easily link-share Drive files within the marketing department, without sharing them with your entire company"
If you did watch the whole Google Workspace Administration Guide, there are 4-5 videos mentioning this, why would you keep using "My Drive" if what you want is to share within a team.. Shared Drive old name is Team Drives so yes, it has to be BC. There is no way E is correct.
upvoted 1 times

RAZKZ 1 year, 9 months ago
I think I miss-understood the structure of the answer.

When choosing B, C, does that mean you do BOTH these actions to achieve the requirement? or EITHER?

In the case of both this makes sense, in the case of EITHER, I would say between B and E, E makes more sense, there is no requirement for restricting access to external, just a requirement for making it "easily link-share Drive files within the marketing department"

This is my first google cert exam, so I'm still trying to get the hand of how they phrase things.
upvoted 2 times

jaxclain 1 year, 8 months ago
Sorry, After reviewing the question a second time, I changed my mind, correct answer is CE, for sure has to be C because Shared Drive is Google best Recommended practices for sharing within Groups or teams.. and Target Audience to avoid these users to share documents internally: https://support.google.com/a/answer/10356781?fl=1#zippy=%2Climit-link-sharing-to-only-employees
upvoted 2 times

coombek2 1 year, 9 months ago

B and C are correct.

--

Why A, D, and E are wrong.

--

Option A involves creating a shared drive that is shared internally organization-wide, which does not restrict sharing to the marketing department.

Option D involves updating the link sharing default for the marketing team, but does not provide a solution for managing the sharing of Drive files.

Option E involves creating a target audience in the admin panel, but does not provide a way to restrict sharing to the marketing department.

upvoted 1 times

RAZKZ 1 year, 9 months ago

They never mentioned to "restrict" to the marketing department.

They mentioned an easy link sharing to the marketing department.

upvoted 1 times

jitu028 1 year, 9 months ago

Correct answer - CE

https://support.google.com/a/users/answer/9310249#1.2

https://support.google.com/a/answer/9935192?hl=en#:~:text=a%20target%20audience-,Create%20a%20target%20audience,as%20Google%20Drive%2C%20to%20make%20it%20availa

Before%20you%20begin

upvoted 2 times

Question #3 *Topic 1*

Your company has a broad, granular IT administration team, and you are in charge of ensuring proper administrative control. One of those teams, the security team, requires access to the Security Investigation Tool. What should you do?

A. Assign the pre-built security admin role to the security team members.

B. Create a Custom Admin Role with the Security Center privileges, and then assign the role to each of the security team members.

C. Assign the Super Admin Role to the security team members.

D. Create a Custom Admin Role with the security settings privilege, and then assign the role to each of the security team members.

Suggested Answer: *B*

Community vote distribution

B (74%) D (26%)

jitu028 Highly Voted 1 year, 9 months ago

Selected Answer: B

Correct answer - B

https://support.google.com/a/answer/9043255#:~:text=To%20give%20access%20only%20to%20the%20investigation%20tool%2C%20chec

upvoted 6 times

jonyuka Most Recent 3 weeks, 2 days ago

Selected Answer: B

B. Create a Custom Admin Role with the Security Center privileges, and then assign the role to each of the security team members.

upvoted 1 times

Laso 10 months, 1 week ago

I think is D, the B option gives more permissions than needed

upvoted 1 times

virat_kohli 10 months, 1 week ago

Selected Answer: B

B. Create a Custom Admin Role with the Security Center privileges, and then assign the role to each of the security team members.

upvoted 1 times

virat_kohli 10 months, 1 week ago

Selected Answer: B

B. Create a Custom Admin Role with the Security Center privileges, and then assign the role to each of the security team members.

upvoted 1 times

marcureli 10 months, 3 weeks ago

D

This setting "Audit & investigation." into Security Center is the one who give access to the Security Investigation Tool. If you give access to the all Security Center , you are giving full access to the Security.

upvoted 1 times

amministrazione 11 months, 3 weeks ago

B. Create a Custom Admin Role with the Security Center privileges, and then assign the role to each of the security team members.

upvoted 1 times

Gomesallef 12 months ago

Selected Answer: B

b pois não é granular é necessário acessar a parte de "segurança inteira".

upvoted 1 times

bond004 1 year ago

Selected Answer: D

D is correct as granular access is mentioned

upvoted 1 times

Jane1234YIP 1 year, 1 month ago

Selected Answer: B

B is correct

upvoted 1 times

BearPop 1 year, 1 month ago

B is correct

https://support.google.com/a/answer/1219251?sjid=9124437181290937081-EU#zippy=%2Csecurity%2Csecurity-center:~:text=Secure%20LDAP-,Security%20Center,-This%20privilege%20is

upvoted 2 times

Bardapapa 1 year, 2 months ago

B is correct

upvoted 1 times

Debbz 1 year, 5 months ago

Selected Answer: D

B is correct

upvoted 2 times

userX100 1 year, 5 months ago

Selected Answer: B

B is correct

upvoted 2 times

barksgw 1 year, 7 months ago

Selected Answer: D

I believe D is correct because with B you would give full access to the Security Center, and the question is only referring to the 'Investigatior

https://support.google.com/a/answer/9043255#:~:text=To%20give%20access%20only%20to%20the%20investigation%20tool%2C%20chec

upvoted 2 times

jaxclain 1 year, 9 months ago

Selected Answer: B

B is correct.

A - there is not a pre-built granular admin role just for security.

C - No need Super Admin

D - Security settings privilege will not give access to the Security Center.

https://support.google.com/a/answer/1219251#api&domains&groups&organization&reports&user_security&support&users&zippy=%2Csecu center

upvoted 1 times

Question #4 *Topic 1*

Your organization has a new security requirement around data exfiltration on iOS devices. You have a requirement to prevent users from copying content from a Google app (Gmail, Drive, Docs, Sheets, and Slides) in their work account to a Google app in their personal account or a third-party app. What steps should you take from the admin panel to prevent users from copying data from work to non-work apps on iOS devices?

A. Navigate to “Data Protection” setting in Google Admin Console's Device management section and disable the “Allow users to copy data to personal apps” checkbox.

B. Disable “Open Docs in Unmanaged Apps” setting in Google Admin Console’s Device management section.

C. Navigate to Devices > Mobile and endpoints > Universal Settings > General and turn on Basic Mobile Management.

D. Clear the “Allow items created with managed apps to open in unmanaged apps” checkbox.

Suggested Answer: *A*

Community vote distribution

A (90%) 10%

jitu028 Highly Voted 1 year, 9 months ago

Selected Answer: A

https://support.google.com/a/answer/6328700?hl=en&ref_topic=6079327#managed_apps&zippy=%2Cdata-actions
Allow users to copy Google Workspace items to personal apps
Allows users to copy content from a Google app (such as Gmail, Drive, Docs, Sheets, Slides, Chat, and Meet) to a Google app in their personal account or a third-party app. Also allows users to drag content between Google apps, for any account.

To prevent users from copying or dragging information from their work account, or using the All inboxes feature (which combines messages from multiple Gmail accounts into one inbox), uncheck the box.

upvoted 8 times

breakkanny 1 year, 9 months ago

Is it valid

upvoted 3 times

emmanuel_katto Most Recent 10 months, 1 week ago

Answer A (Navigate to “Data Protection” setting in Google Admin Console's Device management section and disable the “Allow users to copy data to personal apps” checkbox.)

upvoted 1 times

virat_kohli 10 months, 1 week ago

Selected Answer: A

A. Navigate to “Data Protection” setting in Google Admin Console's Device management section and disable the “Allow users to copy data to personal apps” checkbox.

upvoted 1 times

jcloud965 10 months, 3 weeks ago

Selected Answer: A

Answer is A but the path is wrong.
It should be written Devices>Mobile and endpoints>iOS settings>Data sharing

upvoted 2 times

marcureli 10 months, 3 weeks ago

D Devices -> Mobile and endpoints -> iOS settings -> Data sharing Allow items created with managed apps to open in unmanaged apps
Clear the "Allow items created with managed apps to open in unmanaged apps" checkbox.

upvoted 3 times

amministrazione 11 months, 3 weeks ago

A. Navigate to “Data Protection” setting in Google Admin Console's Device management section and disable the “Allow users to copy data to personal apps” checkbox.

upvoted 1 times

Gomesallef 12 months ago

Selected Answer: A

por eliminações a correta é a "A", pois se tratam de permitir o trafego de dados entre contas.

upvoted 1 times

danaracena 1 year, 1 month ago

Selected Answer: B

Its B. As far as i know the option “Allow users to copy data to personal apps” is a function exclusive to Android Management (preventing the act of "Copy/paste"). The functions available for iOS are the ones related to open documents on managed/non managed apps

upvoted 1 times

wborquez 1 year, 1 month ago

This is the path where the configuration is located:
Devices>Mobile and endpoints>iOS Settings>Share data

upvoted 2 times

BearPop 1 year, 1 month ago

A - Definately https://support.google.com/a/answer/6328700?hl=en?hl=en#zippy=%2Cdata-actions:~:text=Allow%20users%20to%20copy%20Google%20Workspace%20items%20to%20personal%20apps

upvoted 1 times

Orioners 1 year, 2 months ago

Selected Answer: B

Answer is B: https://support.google.com/a/answer/6328700#open_unmanaged&zippy=%2Cabrir-documentos-en-aplicaciones-no-gestionadas%2Copen-docs-in-unmanaged-apps

upvoted 1 times

ferchocolombia 1 year, 3 months ago

Selected Answer: A

A
https://support.google.com/a/answer/6328700?hl=en&ref_topic=6079327#managed_apps&zippy=%2Cdata-actions

upvoted 1 times

Debbz 1 year, 5 months ago

Selected Answer: A

A is correct

upvoted 2 times

blueknight479 1 year, 5 months ago

The answer is B

upvoted 2 times

Passerofexams 1 year, 6 months ago

Selected Answer: A

Kindly see:

https://support.google.com/a/answer/6328700?hl=en#zippy=%2Cdata-actions

upvoted 1 times

jaxclain 1 year, 9 months ago

Selected Answer: A

A seems correct, the other 3 options will not do the job.

upvoted 3 times

Question #5 *Topic 1*

Your organization recently implemented context-aware access policies for Google Drive to allow users to access Drive only from corporate managed desktops. Unfortunately, some users can still access Drive from non-corporate managed machines. What preliminary checks should you perform to find out why the Context-Aware Access policy is not working as intended? (Choose two.)

A. Confirm that the user has a Google Workspace Enterprise Plus license.

B. Delete and recreate a new Context-Aware Access device policy.

C. Check whether device policy application is installed on users' devices.

D. Confirm that the user has at least a Google Workspace Business license.

E. Check whether Endpoint Verification is installed on users' desktops.

Suggested Answer: *CE*

Community vote distribution

AE (74%) CE (26%)

IamSam05 Highly Voted 1 year, 9 months ago

Answer is:- option-A & option-E

upvoted 5 times

HM2H 1 year, 9 months ago

Agree, the first answer should be the Enterprise license (A)

https://support.google.com/a/answer/9275380?hl=en&fl=1

And we need to check whether the end point verification is installed or not (E),

the endpoint verification can be use to filter the approved devices

https://support.google.com/a/answer/9007320?hl=en&fl=1

upvoted 4 times

jdosh Highly Voted 1 year, 3 months ago

Selected Answer: CE

Ent Standard has context-aware and Business licenses don't

upvoted 5 times

Mr_JJ Most Recent 4 months, 3 weeks ago

Selected Answer: AE

The first answer should be the Enterprise license (A) - what if some of the users has business or Ent. Starter?

https://support.google.com/a/answer/9275380

And

Check whether the end point verification is installed or not (E),

the endpoint verification can be used to filter the approved devices. We know it is not necessary, but it is a security compliance + by process of elimination.

https://support.google.com/a/answer/9007320

upvoted 1 times

a17b29d 6 months ago

Why would you need to install something on a users laptop to disallow access? By default no devices would have the software installed. It wouldn't make sense that access would be allowed absent that software.

upvoted 4 times

virat_kohli 10 months, 1 week ago

Selected Answer: AE

A. Confirm that the user has a Google Workspace Enterprise Plus license.

E. Check whether Endpoint Verification is installed on users' desktops.

upvoted 1 times

virat_kohli 10 months, 1 week ago

A. Confirm that the user has a Google Workspace Enterprise Plus license.
E. Check whether Endpoint Verification is installed on users' desktops.
upvoted 1 times

jcloud965 10 months, 3 weeks ago
Selected Answer: AE
The 1st answer should be "Enterprise Standard" or "Enterprise Plus" or "Cloud Identity Premium"
upvoted 4 times

amministrazione 11 months, 3 weeks ago
A. Confirm that the user has a Google Workspace Enterprise Plus license.
E. Check whether Endpoint Verification is installed on users' desktops.
upvoted 1 times

Gomesallef 11 months, 3 weeks ago
Selected Answer: AE
A, E pq é necessario ter o licenciamento e o endpoint verification instalado na maquina.
C,E são a mesma resposta!!!
upvoted 1 times

Steventjie 1 year ago
Selected Answer: AE
Device policy application is for mobile devices. You need either Enterprise licenses (or Business + Cloud Identity Premium licenses) to get this working (A) and the Endpoint Verification extension needs to be installed on the machine's browser.
upvoted 1 times

Jane1234YIP 1 year, 1 month ago
Selected Answer: CE
CE is correct
upvoted 2 times

swiftst 1 year, 4 months ago
How would you enforce installing a verification component on non-corporate-managed devices? This makes no sense. If you can't manage the device you can't put a plugin/etc there. If you manage the device, then there should be no issue.
upvoted 2 times

pgwagopo 1 year, 7 months ago
Selected Answer: AE
AE indeed
upvoted 1 times

ebco_exam 1 year, 8 months ago
AE, indeed
upvoted 1 times

MC2442 1 year, 8 months ago
Selected Answer: AE
AE, dough the extension is pushed to Chrome browser and not on desktop.
upvoted 2 times

jaxclain 1 year, 9 months ago
Selected Answer: AE
100% sure A and E are correct, you need GW Enterprise Plus for Context Aware Access and the Endpoint Verification extension needs to be installed as well, here is the documentation: https://support.google.com/a/users/answer/9018161?hl=en
upvoted 3 times

jdosh 1 year, 2 months ago
Enterprise Standard has Context-Aware so A is not correct.
upvoted 1 times

AmirSBC 1 year, 9 months ago
Selected Answer: AE
https://support.google.com/a/answer/9275380?hl=en&fl=1
https://support.google.com/a/answer/9007320?hl=en&fl=1
upvoted 3 times

Question #6 *Topic 1*

Your organization has enabled spoofing protection against unauthenticated domains. You are receiving complaints that email from multiple partners is not being received. While investigating this issue, you find that emails are all being sent to quarantine due to the configured safety setting. What should be the next step to allow uses to review these emails and reduce the internal complaints while keeping your environment secure?

A. Add your partner domains IPs to the Inbound Gateway setting.

B. Change the spoofing protection to deliver the emails to spam instead of quarantining them.

C. Add your partner sending IP addresses to an allowlist.

D. Change the spoofing protection to deliver the emails to inboxes with a custom warning instead of quarantining them.

Suggested Answer: *D*

Community vote distribution

B (64%) A (19%) Other

jitu028 Highly Voted 1 year, 9 months ago

Selected Answer: B

correct answer - B

https://support.google.com/a/answer/9157861?hl=en#:~:text=Move%20email%20to,with%20this%20action.

upvoted 13 times

Mr_JJ 4 months, 3 weeks ago

C: Users may complain that legitimate emails are landing in their spam folders, requiring them to manually move them to the inbox. Forcing over 10k users to create Gmail filters would be inconvenient. The best approach is to minimize the impact on the user experience.

upvoted 3 times

Mr_JJ Most Recent 4 months, 3 weeks ago

C: Users may complain that legitimate emails are landing in their spam folders, requiring them to manually move them to the inbox. Forcing over 10k users to create Gmail filters would be inconvenient. The best approach is to minimize the impact on the user experience.

upvoted 2 times

virat_kohli 10 months, 1 week ago

Selected Answer: B

B. Change the spoofing protection to deliver the emails to spam instead of quarantining them.

upvoted 1 times

Gomesallef 10 months, 3 weeks ago

Selected Answer: B

correct answer - B

upvoted 1 times

amministrazione 11 months, 3 weeks ago

B. Change the spoofing protection to deliver the emails to spam instead of quarantining them.

upvoted 1 times

AldoSan666 1 year, 1 month ago

Correct answer is - C :

I got wrong the past one, is not A

¨Add IP addresses to allowlists in Gmail

Help prevent messages from certain IP addresses from being marked as spam by adding them to an email allowlist. Messages from these addresses won't be marked as spam by Gmail.

Email allowlists are always applied to your entire domain. You can’t create email allowlists that apply to specific organizational units only.

IP addresses of your mail servers that are forwarding email to Gmail should be added to Inbound Gateway and not in IP allowlist¨

https://support.google.com/a/answer/60751?hl=en
upvoted 4 times

AldoSan666 1 year, 1 month ago
Correct answer is - A :

¨Add IP addresses to allowlists in Gmail

Help prevent messages from certain IP addresses from being marked as spam by adding them to an email allowlist. Messages from these addresses won't be marked as spam by Gmail.

Email allowlists are always applied to your entire domain. You can’t create email allowlists that apply to specific organizational units only.

IP addresses of your mail servers that are forwarding email to Gmail should be added to Inbound Gateway and not in IP allowlist¨

https://support.google.com/a/answer/60751?hl=en
upvoted 1 times

jcloud965 10 months, 3 weeks ago
It says multiple partners : adding them to allowlist is not a good solution
upvoted 2 times

[Removed] 1 year, 1 month ago
Selected Answer: A
A is correct...Sending to spam isn't a viable option for employees who work constantly with the partners, custom warning doesnt keep the environment secure...allowlist doesnt override the quarantine feature but setting up inbound gateway does and it keeps the security configurations tight
upvoted 1 times

jcloud965 10 months, 3 weeks ago
Employees can always mark these email as non spam
upvoted 2 times

wborquez 1 year, 1 month ago
Selected Answer: B
Quarantine action: When you select Quarantine for any of the advanced security settings, the quarantine you select applies only to incoming messages. This is true even when the quarantine you select specifies actions to take on outgoing messages. <Allowlist settings don't override the Quarantine option.
Warning banners: Warning banners (yellow box) appear only in Gmail web. <Third-party apps do not display a warning banner.
Other spam settings: These advanced security features work independently of other spam settings you might have previously turned on. For example, even if you've listed a domain as a safe sender in spam settings, the enhanced security features are still applied.

https://support.google.com/a/answer/9157861?hl=en#:~:text=Move%20email%20to,with%20this%20action.
upvoted 1 times

Orioners 1 year, 2 months ago
Selected Answer: C
la respuesta es C: https://support.google.com/a/answer/60751?hl=en&sjid=14509679687775256174-SA
upvoted 4 times

jdosh 1 year, 2 months ago
Selected Answer: B
B, the key thing is letting the user review but remain secure.
upvoted 2 times

swiftst 1 year, 4 months ago
Selected Answer: D

Users don't look at spam. The custom warning label is much more functional in the real world

upvoted 2 times

swiftst 1 year, 4 months ago

Users don't look at spam. The custom warning label is much more functional in the real world.

upvoted 1 times

userX100 1 year, 5 months ago

Selected Answer: B

B. Change the spoofing protection to deliver the emails to spam instead of quarantining them.

upvoted 1 times

barksgw 1 year, 6 months ago

Selected Answer: B

Messages that aren’t authenticated with DMARC by the receiving server are sent to the recipient’s spam folder. If the receiving mail server h
options:~:text=Messages%20that%20aren%E2%80%99t%20authenticated%20with%20DMARC%20by%20the%20receiving%20server%20(

upvoted 1 times

ssa1983 1 year, 7 months ago

D is not correct because there is no custom warning

C would keep the complaints ongoing

A would still process those messages for spam/spoofing checks and thus quarantine them

C is the only solution in my opinion

upvoted 3 times

NadiaOne 1 year, 7 months ago

The correct answer is B.

The D one is not correct because it states "custom warning message": you cannot customize the warning message for the Advanced Phishing and Malware Protection section in the Admin console.

upvoted 1 times

Question #7 *Topic 1*

As the Workspace Administrator, you have been asked to delete a temporary Google Workspace user account in the marketing department. This user has created Drive documents in My Documents that the marketing manager wants to keep after the user is gone and removed from Workspace. The data should be visible only to the marketing manager. As the Workspace Administrator, what should you do to preserve this user's Drive data?

A. In the user deletion process, select “Transfer” in the data in other apps section and add the manager's email address.

B. Use Google Vault to set a retention period on the OU where the users reside.

C. Before deleting the user, add the user to the marketing shared drive as a contributor and move the documents into the new location.

D. Ask the user to create a folder under MyDrive, move the documents to be shared, and then share that folder with the marketing team manager.

Suggested Answer: *C*

Community vote distribution

A (100%)

jitu028 Highly Voted 1 year, 9 months ago

Selected Answer: A

Correct Answer - A

https://support.google.com/a/answer/6223444?hl=en#zippy=%2Ctransfer-user-drive-or-google-data:~:text=You%20can%20transfer,Tap%20Transfer.

upvoted 14 times

woodenhoe Most Recent 2 months ago

Isn't C the wrong choice because members of the shared drive would have access to the files?

upvoted 1 times

Mr_JJ 4 months, 3 weeks ago

Selected Answer: A

Correct Answer - A

https://support.google.com/a/answer/6223444

upvoted 1 times

virat_kohli 10 months, 1 week ago

Selected Answer: A

A. In the user deletion process, select “Transfer” in the data in the other apps section and add the manager's email address.

upvoted 1 times

jcloud965 10 months, 3 weeks ago

Selected Answer: A

A : Transfer ownership using the bultin tool during the user deletion process

upvoted 1 times

Gomesallef 10 months, 3 weeks ago

Selected Answer: A

Correct Answer - A

upvoted 1 times

Chentimiento 10 months, 3 weeks ago

CORRECT ANSWER WOULD BE A, WHICH IS TO TRANSFER THE DATA BEFORE DELETING THE USER

upvoted 1 times

amministrazione 11 months, 3 weeks ago

A. In the user deletion process, select “Transfer” in the data in other apps section and add the manager's email address.

upvoted 1 times

Eagles215Philly 1 year ago

Selected Answer: A

Beluieve the Answer is A. Moving the docuemnts to the Marketing Share Drive would mean MULTIPLE people would have access to the files. In the question it says that only his manager should have access.

upvoted 1 times

Steventjie 1 year ago

Guys, who vets these answers? How can I trust this when the overwhelming community consensus is that the correct answer is something else? I need to pass this exam. Where can I go to get a proper, up-to-date mock exam with answers?

upvoted 3 times

AldoSan666 1 year, 1 month ago

Only answer that matches Admin.Google.com is A

upvoted 1 times

Orioners 1 year, 2 months ago

Selected Answer: A

Correct Answer - A: https://support.google.com/a/answer/6223444?hl=en#zippy=%2Ctransfer-user-drive-or-google-data

upvoted 2 times

jdosh 1 year, 3 months ago

Selected Answer: A

No mention in the question that there is a current marketing shared drive and the manager is the only member of it. To be on the safe side letter A should be the answer.

upvoted 2 times

Twindaddy 1 year, 7 months ago

How is C restricting access only to the manager (unless only the manager has access to that shared drive?). I say it's A.

upvoted 3 times

jaxclain 1 year, 9 months ago

Selected Answer: A

I will also vote for A but the question is confusing because it says that the user created Drive documents in My Documents but we have to assume the My Documents folder is inside his Drive lol

upvoted 3 times

Question #8 *Topic 1*

As a Google Workspace administrator for your organization, you are tasked with controlling which third-party apps can access Google Workspace data. Before implementing controls, as a first step in this process, you want to review all the third-party apps that have been authorized to access Workspace data. What should you do?

A. Open Admin Console > Security > API Controls > App Access Control > Manage Third Party App Access.

B. Open Admin Console > Security > API Controls > App Access Control > Manage Google Services.

C. Open Admin Console > Security > Less Secure Apps.

D. Open Admin Console > Security > API Controls > App Access Control > Settings.

Suggested Answer: *A*

Community vote distribution

A (100%)

jitu028 Highly Voted 1 year, 9 months ago

Selected Answer: A

Correct Answer - A

https://support.google.com/a/answer/7281227?hl=en#zippy=%2Cstep-manage-third-party-app-access-to-google-services-add-apps:~:text=In%20the%20Admin,App%20Access.

upvoted 7 times

virat_kohli Most Recent 10 months, 1 week ago

Selected Answer: A

A. Open Admin Console > Security > API Controls > App Access Control > Manage Third Party App Access.

upvoted 1 times

Gomesallef 10 months, 4 weeks ago

Selected Answer: A

Correct Answer - A

upvoted 1 times

amministrazione 11 months, 3 weeks ago

A. Open Admin Console > Security > API Controls > App Access Control > Manage Third Party App Access.

upvoted 1 times

Gomesallef 11 months, 3 weeks ago

Selected Answer: A

Correct Answer - A

https://support.google.com/a/answer/7281227?hl=en#zippy=%2Cstep-manage-third-party-app-access-to-google-services-add-apps:~:text=In%20the%20Admin,App%20Access.

upvoted 1 times

jaxclain 1 year, 9 months ago

Selected Answer: A

There is a similar question with App Access Control besides this so for sure A is correct.

upvoted 1 times

Question #9 *Topic 1*

Your organization wants more visibility into actions taken by Google staff related to your data for audit and security reasons. They are specifically interested in understanding the actions performed by Google support staff with regard to the support cases you have opened with Google. What should you do to gain more visibility?

A. From Google Admin Panel, go to Audit, and select Access Transparency Logs.

B. From Google Admin Panel, go to Audit, and select Login Audit Log.

C. From Google Admin Panel, go to Audit, and select Rules Audit Log.

D. From Google Admin Panel, go to Audit, and select Admin Audit Log.

Suggested Answer: *D*

Community vote distribution

A (100%)

pamcanova Highly Voted 1 year, 9 months ago

Selected Answer: A

Google staff logs related to accessing user content are stored in Access Transparency logs

https://support.google.com/a/answer/9230474?hl=en

upvoted 11 times

virat_kohli Most Recent 10 months, 1 week ago

Selected Answer: A

A. From the Google Admin Panel, go to Audit, and select Access Transparency Logs.

upvoted 2 times

amministrazione 11 months, 3 weeks ago

A. From Google Admin Panel, go to Audit, and select Access Transparency Logs.

upvoted 1 times

Gomesallef 11 months, 3 weeks ago

Selected Answer: A

"Como administrador da sua organização, você pode usar a ferramenta de investigação de segurança para executar pesquisas relacionadas aos eventos de registro de transparência no acesso. Lá você pode visualizar um registro de ações que fornece informações sobre as ações da equipe do Google quando acessam seus dados." https://support.google.com/a/answer/9230979

upvoted 1 times

andicpl 1 year, 2 months ago

Ist 100% A!!!! Nobody changing the answers here???!!!!!!!! Shit

upvoted 1 times

barksgw 1 year, 3 months ago

Selected Answer: A

"As your organization's administrator, you can use the security investigation tool to run searches related to Access Transparency log events. There you can view a record of actions that provide information about the actions of Google staff when they access your data." https://support.google.com/a/answer/9230979

upvoted 1 times

dadewole 1 year, 8 months ago

but the path listed in option A is not thesame with the path needed to access Access Transparency log events

https://support.google.com/a/answer/9230979

upvoted 1 times

Gomesallef 11 months, 3 weeks ago

na verdade é sim, se vc mexer na ferramente vai perceber que ele altera a opção do "ferramenta de investigação" para " Auditoria e investigação"

upvoted 1 times

jaxclain 1 year, 9 months ago

Selected Answer: A

I also agree with pamcanova, Access Transparency Logs will provide the required visibility.

upvoted 2 times

Question #10 *Topic 1*

Your organization recently had a sophisticated malware attack that was propagated through embedded macros in email attachments. As a Workspace administrator, you want to provide an additional layer of anti-malware protection over the conventional malware protection that is built into Gmail. What should you do to protect your users from future unknown malware in email attachments?

A. Run queries in Security Investigation Tool.

B. Turn on advanced phishing and malware protection.

C. Enable Security Sandbox.

D. Enable Gmail confidential mode.

Suggested Answer: *B*

Community vote distribution

C (76%) B (24%)

jitu028 Highly Voted 1 year, 9 months ago

Selected Answer: C

Answer - C

https://support.google.com/a/answer/7676854?hl=en#zippy=%2Cscan-all-attachments-in-security-sandbox:~:text=detect%20harmful%20attachments-,Set%20up%20rules%20to%20detect%20harmful%20attachments,Security%20Sandbc

Supported%20editions%20for

upvoted 7 times

Nico282 Most Recent 8 months, 4 weeks ago

Selected Answer: C

https://support.google.com/a/answer/7676854

Security Sandbox is used to scan Microsoft Office files, a.k.a. the ones with the embedded macros.

upvoted 2 times

Nico282 9 months ago

Selected Answer: C

Email attachments can include malicious software that might be missed by traditional antivirus programs. To identify these threats, Gmail can scan or run attachments in a virtual environment called Security Sandbox.

File types scanned in Security Sandbox include Microsoft executables, Microsoft Office, and PDF.

https://support.google.com/a/answer/7676854?hl=en

upvoted 2 times

virat_kohli 10 months, 1 week ago

Selected Answer: C

C. Enable Security Sandbox.

upvoted 1 times

virat_kohli 10 months, 1 week ago

Selected Answer: C

C. Enable Security Sandbox.

upvoted 1 times

amministrazione 11 months, 3 weeks ago

C. Enable Security Sandbox.

upvoted 1 times

Gomesallef 11 months, 3 weeks ago

Selected Answer: B

B is correct, configurações de phising e malwere estão em gamil -> compliance & security

upvoted 1 times

Stiflersammy 1 year ago
The answer is B https://support.google.com/a/answer/9157861?hl=en
upvoted 1 times

Chan1010 1 year ago
C is Correct
Deep Gmail scans. Enhanced pre-delivery scanning of incoming email is automatically enabled to identify phishing attempts. Also, for Enterprise users the security sandbox feature is turned on to provide deep scanning of attachments for unknown malware.
upvoted 1 times

[Removed] 1 year, 1 month ago
Selected Answer: B
Correct answer is B. It enables the use of physical security keys...physical security keys are not built into gmail, sandbox is
upvoted 1 times

Jane1234YIP 1 year, 1 month ago
Selected Answer: C
C is correct
Enabling the Security Sandbox feature adds an extra layer of protection against unknown or zero-day malware threats in email attachments. The Security Sandbox feature opens suspicious attachments in a secure and isolated environment, which helps prevent potential malware from affecting the user's device or the organization's network.
upvoted 1 times

BearPop 1 year, 1 month ago
C - Security Sandbox
upvoted 1 times

jerichoOrtega 1 year, 2 months ago
Selected Answer: B
"Security sandbox provides an additional level of anti-malware protection over and above conventional detection."
- Google Blog
https://workspaceupdates.googleblog.com/2019/04/gmail-security-sandbox-advanced-malware-protection.html
upvoted 2 times

jerichoOrtega 1 year, 2 months ago
Misclick, it should be C
upvoted 1 times

jdosh 1 year, 3 months ago
Selected Answer: B
It clearly says other than the built-in conventional anti-malware of Gmail. Sandbox is built-in to Gmail.
upvoted 2 times

Passerofexams 1 year, 5 months ago
Selected Answer: C
https://support.google.com/a/answer/9378686?hl=en

As mentioned previously
upvoted 1 times

Umesh_Jadhav 1 year, 6 months ago
Selected Answer: C
C is correct
upvoted 1 times

kamlcloud 1 year, 7 months ago
B is the right, because security sandbox is used for zero day threats, something that is not yet known as malware, however the question talks about the "conventional" malware protection that is "built into Gmail".
upvoted 1 times

Question #11 *Topic 1*

Your organization's information security team has asked you to determine and remediate if a user (user1@example.com) has shared any sensitive documents outside of your organization. How would you audit access to documents that the user shared inappropriately?

A. Open Security Investigation Tool-> Drive Log Events. Add two conditions: Visibility Is External, and Actor Is user1@example.com.

B. Have the super administrator use the Security API to audit Drive access.

C. As a super administrator, change the access on externally shared Drive files manually under user1@example.com.

D. Open Security Dashboard-> File Exposure Report-> Export to Sheet, and filter for user1@example.com.

Suggested Answer: *C*

Community vote distribution

A (88%) 12%

impearl Highly Voted 1 year, 9 months ago

Answer - A
https://support.google.com/a/answer/11480192?hl=en&ref_topic=11479095#:~:text=View%20files%20shared,Click%20Search.
upvoted 13 times

nisha31011990 1 year, 9 months ago

is this the actual exam question and has been updated recently ?
upvoted 3 times

jaxclain Highly Voted 1 year, 9 months ago

Selected Answer: A

Option C is not correct lol, read the question again... "HOW would you audit access to documents", for this purpose GW has a feature called Investigation Tool... not everyone knows how to use it but you can for sure get the report, also recently GW updated the Audits and now its merged Audits / Investigation tool so you already have 2 reasons why option A is correct lol, why would you pick option C.. is not asking you to change the external access.. is asking you to Audit.. here is the documentation: https://support.google.com/a/answer/9300435?hl=en

Also I have worked as a GW Admin and Deployment for about 7 years so I know perfectly that the Investigation tool can be used for this.
upvoted 9 times

virat_kohli Most Recent 10 months, 1 week ago

Selected Answer: A

A. Open Security Investigation Tool-> Drive Log Events. Add two conditions: Visibility Is External, and Actor Is user1@example.com.
upvoted 2 times

amministrazione 11 months, 3 weeks ago

A. Open Security Investigation Tool-> Drive Log Events. Add two conditions: Visibility Is External, and Actor Is user1@example.com.
upvoted 1 times

Gomesallef 11 months, 3 weeks ago

Selected Answer: A

Letter A, he is asking to investigate and not change settings.
upvoted 1 times

Steventjie 1 year ago

Selected Answer: A

D does not address auditing what the user has shared externally, only to turn off their ability to do so, this cannot be correct.
upvoted 1 times

BearPop 1 year, 1 month ago

Answer A
https://support.google.com/a/answer/11480192?hl=en&ref_topic=11479095#:~:text=View%20files%20shared,Click%20Search.

upvoted 1 times

userX100 1 year, 5 months ago

Selected Answer: A

A is correct

upvoted 2 times

Umesh_Jadhav 1 year, 6 months ago

Selected Answer: A

A is correct ans

upvoted 2 times

RAZKZ 1 year, 9 months ago

Selected Answer: A

Seems like the answer is A (to trace, BUT IT DOES NOT REMEDIATE):
https://support.google.com/a/answer/11480192?hl=en&ref_topic=11479095#:~:text=View%20files%20shared,Click%20Search.

These questions are so weird...

upvoted 3 times

Exam__ 1 year, 9 months ago

Selected Answer: A

Answer - A

upvoted 2 times

testseb 1 year, 9 months ago

It is A. The option that is exported in answer D doesn't show user names

upvoted 2 times

jitu028 1 year, 9 months ago

Selected Answer: C

Answer - C
https://support.google.com/a/answer/60781?
hl=en#:~:text=If%20you%20turn%20off%20external%20sharing%2C%20users%20can%E2%80%99t%20share%20the%20following%20ite

upvoted 3 times

Question #12 *Topic 1*

A user is reporting that external, inbound messages from known senders are repeatedly being incorrectly classified as spam. What steps should the admin take to prevent this behavior in the future?

A. Modify the SPF record for your internal domain to include the IPs of the external user's mail servers.

B. Update the spam settings in the Admin Console to be less aggressive.

C. Add the sender's domain to an allowlist via approved senders in the Admin Console.

D. Instruct the user to add the senders to their contacts.

Suggested Answer: *A*

Community vote distribution

C (95%) 5%

jitu028 Highly Voted 1 year, 9 months ago

Selected Answer: C

Correct Answer - C

https://support.google.com/a/answer/60752?hl=en#:~:text=Approved%20senders%20list%E2%80%94,settings%20in%20Google%20Workspace.

upvoted 9 times

virat_kohli Most Recent 10 months, 1 week ago

Selected Answer: C

C. Add the sender's domain to an allowlist via approved senders in the Admin Console.

upvoted 2 times

amministrazione 11 months, 3 weeks ago

C. Add the sender's domain to an allowlist via approved senders in the Admin Console.

upvoted 2 times

Gomesallef 11 months, 3 weeks ago

Selected Answer: C

Correct letter C

https://support.google.com/a/answer/60752?hl=en#:~:text=Approved%20senders%20list%E2%80%94,settings%20in%20Google%20Workspace.

upvoted 2 times

Steventjie 1 year ago

SPF is used to indicate which mail servers are allowed to send emails from YOUR domain and has nothing to do with external, inbound emails. Where are these answers derived from, Google? Can't be.

upvoted 3 times

[Removed] 1 year, 1 month ago

Selected Answer: C

C is correct

upvoted 1 times

BearPop 1 year, 1 month ago

Answer - C

upvoted 1 times

RubyMug 1 year, 2 months ago

Answer - A

It's not about the domain but about setting with IP....

https://support.google.com/a/answer/60752?hl=en&sjid=15145020688457694065-AP

upvoted 1 times

Stiflersammy 1 year ago

What if the person is working from outside of the office and the IP changes will the email still deliver?

upvoted 1 times

userX100 1 year, 5 months ago

Selected Answer: C

C- Correct

upvoted 1 times

Willem_M 1 year, 8 months ago

Selected Answer: B

It clearly states "external, inbound messages from known senders are repeatedly" so you do not know what to add to your allowlist in this case? It seems to me that the option "Be more agressieve when filtering spam" is on and should be turned off.

upvoted 1 times

MC2442 1 year, 8 months ago

Selected Answer: C

C: changing spf is for outbound management of authentication.

upvoted 2 times

jaxclain 1 year, 9 months ago

Selected Answer: C

Nothing to add, C is the only correct answer

upvoted 1 times

AsakuraYoh 1 year, 9 months ago

Selected Answer: C

The Answer is C

upvoted 2 times

Question #13 *Topic 1*

The credentials of several individuals within your organization have recently been stolen. Using the Google Workspace login logs, you have determined that in several cases, the stolen credentials have been used in countries other than the ones your organization works in. What else can you do to increase your organization's defense-in-depth strategy?

A. Implement an IP block on the malicious user's IPs under Security Settings in the Admin Console.

B. Use Context-Aware Access to deny access to Google services from geo locations other than the ones your organization operates in.

C. Enforce higher complexity passwords by rolling it out to the affected users.

D. Use Mobile device management geo-fencing to prevent malicious actors from using these stolen credentials.

Suggested Answer: *B*

Community vote distribution

B (100%)

jitu028 Highly Voted 1 year, 9 months ago

Selected Answer: B

Correct answer - B

https://support.google.com/a/answer/9262032?hl=en#zippy=%2Cdefine-access-levelsbasic-mode:~:text=This%20example%20shows%20an%20access%20level%20called%20%E2%80%9Ccorp_access.%E2%80%9D%20If%20%E

upvoted 8 times

JessiePiper Most Recent 3 months, 4 weeks ago

I understand that B is the best answer here, however, isn't Context-Aware Access only available to Enterprise users? What is the best play if they do not have an Enterprise account?

upvoted 1 times

virat_kohli 10 months, 1 week ago

Selected Answer: B

B. Use Context-Aware Access to deny access to Google services from geo locations other than the ones your organization operates in.

upvoted 1 times

amministrazione 11 months, 3 weeks ago

B. Use Context-Aware Access to deny access to Google services from geo locations other than the ones your organization operates in.

upvoted 1 times

BearPop 1 year, 1 month ago

Selected Answer: B

Definately Context Aware Access

upvoted 1 times

gordonchen8998 1 year, 3 months ago

Selected Answer: B

Use Content Aware Access rules to set Geo location for the contries that your users access from, and assign the rules to restrict the access to all the Google WorkSpace services.

upvoted 1 times

userX100 1 year, 5 months ago

Selected Answer: B

B. Use Context-Aware Access to deny access to Google services from geo locations other than the ones your organization operates in.

upvoted 1 times

Mohitpandey 1 year, 8 months ago

Selected Answer: B

B is correct

upvoted 1 times

jaxclain 1 year, 9 months ago

Selected Answer: B

Easy question.. Correct answer is B

upvoted 1 times

HEA22 1 year, 9 months ago

Selected Answer: B

B makes sense

upvoted 3 times

Question #14 *Topic 1*

You are the Workspace administrator for an international organization with Enterprise Plus Workspace licensing. A third of your employees are located in the United States, another third in Europe, and the other third geographically dispersed around the world. European employees are required to have their data stored in Europe. The current OU structure for your organization is organized by business unit, with no attention to user location. How do you configure Workspace for the fastest end user experience while also ensuring that European user data is contained in Europe?

A. Configure a data region at the top level OU of your organization, and set the value to “Europe”.

B. Add three additional OU structures to designate location within the current OU structure. Assign the corresponding data region to each.

C. Configure a configuration group for European users, and set the data region to “Europe”.

D. Configure three configuration groups within your domain. Assign the appropriate data regions to each corresponding group, but assign no preference to the users outside of the United States and Europe.

Suggested Answer: *A*

Community vote distribution

C (70%) A (30%)

RJRF503 Highly Voted 1 year, 9 months ago

Selected Answer: C

Correct answer - C

https://support.google.com/a/answer/7630496?hl=en#zippy=%2Cstep-set-the-organizational-structure

"put them in a configuration group (to set for users across or within departments)".

upvoted 12 times

Aj_yan Most Recent 9 months, 2 weeks ago

Tried to pass this exam 2 weeks ago.

I learned all 95 questions and answers and selected them during exam.

Not passed.

About 80% was from VCE Exam Simulator.

I checked all questions here and they are the same like in VCE with the same answers.

Seems need to use answers that voted by people, nor provided by system.

upvoted 3 times

0dissey_ 9 months, 1 week ago

Hello! I'm sad to hear that you didn't pass the exam because it's waiting for me tomorrow, but I immediately noticed that the system usually gives incorrect answers, so I read all the discussions and remember them exclusively. And in general, what can you say in terms of complexity? Thank you in advance)

upvoted 1 times

Aj_yan 9 months ago

In general, the exam is not difficult, and all 95 questions that are available can be studied with answers in a couple of days.

The main thing is that the answers are correct))).

Did you pass exam?

upvoted 1 times

capilona2 9 months ago

How was your exam? Can you tell us anything on the questions and the answers the system offers?

upvoted 1 times

Aj_yan 9 months ago

in the exam, about 70% of the questions were exactly the same as what we see here

and the order of answers was the same

I purchased Contributor access for 1 month and am now studying the most voted answers.

I think this is the best site for exam preparation.

upvoted 4 times

examprof 9 months ago

@Aj_yan can you please confirm that the QUESTIONS and ALTERNATIVES are the same found here? I'm deeply sorry for your failure. I understand your point and have seen several people here complaining about the inaccuracy of system-generated answers and recommending them to be removed at all. The contributors' most voted answers are the ones to be considered.

upvoted 2 times

virat_kohli 10 months, 1 week ago

Selected Answer: C

C. Configure a configuration group for European users, and set the data region to “Europe”.

upvoted 2 times

amministrazione 11 months, 3 weeks ago

C. Configure a configuration group for European users, and set the data region to “Europe”.

upvoted 1 times

Gomesallef 11 months, 3 weeks ago

Selected Answer: C

Resposta correta - C https://support.google.com/a/answer/7630496?hl=en#zippy=%2Cstep-set-the-organizational-structure

upvoted 1 times

Dido75 12 months ago

C Because The current OU structure for your organization is organized by business unit, with no attention to user location.

upvoted 1 times

topnode2023 1 year ago

Selected Answer: A

Less latency if everyone's data is in the same region - "Europe".

upvoted 1 times

Steventjie 1 year ago

Selected Answer: A

The reason why this probably is A is because, the question indicates that where the data is stored for the non-European employees is irrelevant, thus you might as well change everybody's data to be kept in Europe. No need for OU configuration additions or changes, that's the simplest route.

upvoted 2 times

[Removed] 1 year, 1 month ago

Selected Answer: A

Selecting a specific region doesn't provide performance improvements or fine-tuning for your network or data access. Take the following factors into consideration before making your decision:

Users outside the region where their data is located might experience higher latency in some cases. Latency could happen while:

Editing shared objects in real time across regions
Sharing files, such as documents, with someone outside the user's region
Traveling internationally
From rjrf503 link...so for the fastest user experience the data region should just be europe for the entire organization

upvoted 4 times

BearPop 1 year, 1 month ago

Answer - C

upvoted 1 times

andicpl 1 year, 2 months ago

C - because they asked for the "FASTEST" experience!

upvoted 3 times

jdosh 1 year, 3 months ago

Selected Answer: A

A is correct. It seems like people here are missing the "best user experience" part of the question. The users will have the best experience with sharing, collaboration etc. if all of them are in one region and since the US and other countries do not have a preference it doesn't matter where their data lives.

upvoted 3 times

userX100 1 year, 5 months ago

Selected Answer: C

C is correct

upvoted 2 times

jaxclain 1 year, 8 months ago

Selected Answer: C

C is correct, I forgot to place a comment here, since you only want to modify the Europe employees, then just create a Group for them and set the data region to Europe. The rest will remain the same.

upvoted 4 times

HEA22 1 year, 9 months ago

Selected Answer: C

B can also be Valid answer but it seems they ask only for europe configuration. So i'd go for C

upvoted 3 times

testseb 1 year, 9 months ago

Selected Answer: C

Not all OU's need to be set to Europe; so C

upvoted 2 times

jitu028 1 year, 9 months ago

changing my answer to 'C'

upvoted 2 times

nisha31011990 1 year, 9 months ago

HI JITU, are these the updated actual exam questions ?

upvoted 1 times

Willem_M 1 year, 9 months ago

I can confirm these are up to date (took the exam 2 weeks ago)

upvoted 1 times

RAZKZ 1 year, 9 months ago

Willem, are the answers voted by people reasonable in your opinion?

upvoted 1 times

Willem_M 1 year, 8 months ago

I think about 80-85% of the time I think the majority of the votes are in line with what I believe to be correct, but I can also be wrong ofc!

upvoted 1 times

AsakuraYoh 1 year, 9 months ago

how many % do you think appears on the examination? Thanks

upvoted 1 times

Question #15 *Topic 1*

As a team manager, you need to create a vacation calendar that your team members can use to share their time off. You want to use the calendar to visualize online status for team members, especially if multiple individuals are on vacation What should you do to create this calendar?

A. Request the creation of a calendar resource, configure the calendar to “Auto-accept invitations that do not conflict,” and give your team “See all event details” access.

B. Create a secondary calendar under your account, and give your team “Make changes to events” access.

C. Request the creation of a calendar resource, configure the calendar to “Automatically add all invitations to this calendar,” and give your team “See only free/busy” access.

D. Create a secondary calendar under your account, and give your team “See only free/busy” access.

Suggested Answer: *C*

Community vote distribution

B (76%) C (24%)

jaxclain Highly Voted 1 year, 9 months ago

Selected Answer: B

I have been a Google Workspace Administrator / Deployment for about 7 years lol so I can guarante you option A and C are not right, Calendar Resource is not intented for this purpose, so we are left with option B or D, the only difference between both is to allow members to make changes or not so according to the question "You need a Vacation Calentar that your team members can use to share their time off" meaning they will need editing permissions to the Calendar, meaning? the only viable option is B.
Also if you need documentation, here is the article, mentioning "Track team members’ vacations schedules and business trip dates.":
https://support.google.com/a/users/answer/9308965?hl=en

upvoted 17 times

Nico282 Most Recent 8 months, 4 weeks ago

Selected Answer: B

https://support.google.com/a/users/answer/13293412 and scroll to "Create a Team Calendar":

upvoted 3 times

amministrazione 11 months, 3 weeks ago

B. Create a secondary calendar under your account, and give your team “Make changes to events” access.

upvoted 2 times

topnode2023 1 year ago

Selected Answer: B

Tip from Google to create a "Team Calendar":
https://support.google.com/a/users/answer/13293412?hl=en#zippy=%2Clearn-how

upvoted 2 times

bobsmith69 1 year ago

Selected Answer: C

C- https://support.google.com/a/answer/60765?hl=en

upvoted 1 times

BearPop 1 year, 1 month ago

Selected Answer: B

Tough one - but I would go B

upvoted 1 times

RubyMug 1 year, 2 months ago

Selected Answer: C

Answer C
https://support.google.com/a/answer/60765?hl=en

upvoted 2 times

jdosh 1 year, 3 months ago

Selected Answer: C

C is the best way to go. The manager just wants to see and view the leaves. All the leave filers should just do is add the resource calendar to their leave events. If you do letter B, all other users can see each other leave details and may modify others.

upvoted 2 times

userX100 1 year, 5 months ago

Selected Answer: B

B - Create a secondary calendar under your account, and give your team “Make changes to events” access.

upvoted 1 times

AsakuraYoh 1 year, 9 months ago

Selected Answer: B

Best answer is B

upvoted 1 times

testseb 1 year, 9 months ago

C seem like a solution; but they can never make any changes; Also it should not be a resource it you ask me. I think B is a better solution

upvoted 2 times

jitu028 1 year, 9 months ago

Selected Answer: C

Correct answer - C

https://support.google.com/a/answer/1034381?hl=en#:~:text=Automatically%20add%20all%20invitations%20to%20this%20calendar%E2%80%94All%20invitations%20show%20up%20or

upvoted 3 times

Salman7878 1 year, 9 months ago

Please also review Question 48,49,50

upvoted 3 times

jdosh 1 year, 2 months ago

there is no question 48,49 and 50

upvoted 1 times

Question #16 *Topic 1*

Your Finance team has to share quarterly financial reports in Sheets with an external auditor. The external company is not a Workspace customer and allows employees to access public sites such as Gmail and Facebook. How can you provide the ability to securely share content to collaborators that do not have a Google Workspace or consumer (Gmail) account?

A. Allow external sharing with the auditor using the 'Trusted Domains' feature.

B. Enable the 'Visitor Sharing' feature, and demonstrate it to the Finance team.

C. Use the 'Publish' feature in the Sheets editor to share the contents externally.

D. Attach the Sheet file to an email message, and send to the external auditor.

Suggested Answer: *D*

Community vote distribution

B (80%) D (20%)

jitu028 Highly Voted 1 year, 9 months ago

Selected Answer: B

Correct answer - B

https://support.google.com/drive/answer/9195194?hl=en#:~:text=Share%20with%20visitors,with%20one%20visitor.

upvoted 9 times

virat_kohli Most Recent 10 months, 1 week ago

Selected Answer: B

B. Enable the 'Visitor Sharing' feature, and demonstrate it to the Finance team.

upvoted 2 times

Gomesallef 10 months, 3 weeks ago

Selected Answer: B

Correct answer - B

upvoted 1 times

amministrazione 11 months, 3 weeks ago

B. Enable the 'Visitor Sharing' feature, and demonstrate it to the Finance team.

upvoted 1 times

Eagles215Philly 1 year ago

Selected Answer: D

I believe the answer should be D. From the Sheet, go to FILE->EMAIL->EMAIL THIS FILE. You can send the file to an email address as a PDF, Excel or a Open Document. If you used Visitor Sharing, the users would be able to edit and comment on the sheet. To be more secure you should send the document to the user through email.

upvoted 2 times

Eagles215Philly 1 year ago

I believe the answer should be D. From the Sheet, go to FILE->EMAIL->EMAIL THIS FILE. You can send the file to an email address as a PDF, Excel or a Open Document. If you used Visitor Sharing, the users would be able to edit and comment on the sheet. To be more secure you should send the document to the user through email.

upvoted 1 times

BearPop 1 year, 1 month ago

Answer - B

upvoted 1 times

danaracena 1 year, 2 months ago

Selected Answer: D

Think on the case; The case is a Financial Team, sharing with an external Finance AUDITOR.

The regular figure to share for auditions (more if are finance) is to share "local" files, not collaboration files even if they have Google Accounts. So i think for this case, indeed the proper and most realistic workflow will include the attachment

upvoted 2 times

baha2 1 year, 3 months ago

Selected Answer: B

that do not have a Google Workspace or consumer (Gmail) account

upvoted 1 times

gordonchen8998 1 year, 3 months ago

Selected Answer: B

https://support.google.com/drive/answer/9195194?hl=en#zippy=%2Cfile-types-you-can-share-with-a-non-google-domain

upvoted 1 times

onlyrichard 1 year, 4 months ago

Hi guys, if this is a condition "allows employees to access public sites such as Gmail" why you need to use the Visitor Sharing feature? Just send an email to their gmail account, rigth?

upvoted 1 times

baner911 1 year, 4 months ago

the questions says they don have consumer (Gmail) account

upvoted 1 times

jaxclain 1 year, 9 months ago

Selected Answer: B

Visitor Sharing is ok so B seems correct,

upvoted 2 times

Question #17 *Topic 1*

Your organization has noticed several incidents of accidental oversharing inside the organization. Specifically, several users have shared sensitive Google Drive items with the entire organization by clicking ‘anyone in this group with this link can view’. You have been asked by senior management to help users share more appropriately and also to prevent accidental oversharing to the entire organization. How would you best accomplish this?

A. Create groups, add users accordingly, and educate users on how to share to specific groups of people.

B. Disable sharing to the entire organization so that users must consciously add every person who needs access.

C. Determine sharing boundaries for users that work with sensitive information, and then implement target audiences.

D. Temporarily disable the Google Drive service for individuals who continually overshare.

Suggested Answer: *B*

Community vote distribution

C (76%) A (19%) 5%

jitu028 Highly Voted 1 year, 9 months ago

Selected Answer: C

Answer - C

https://support.google.com/a/answer/9934697?hl=en#zippy=:~:text=Why%20use%20target,for%20broad%20sharing.

upvoted 8 times

virat_kohli Most Recent 10 months, 1 week ago

Selected Answer: C

C. Determine sharing boundaries for users that work with sensitive information, and then implement target audiences.

upvoted 2 times

dija123 10 months, 3 weeks ago

Selected Answer: B

B only can prevent accidental oversharing

upvoted 1 times

Gomesallef 10 months, 3 weeks ago

Selected Answer: C

Answer - C

upvoted 1 times

amministrazione 11 months, 3 weeks ago

C. Determine sharing boundaries for users that work with sensitive information, and then implement target audiences.

upvoted 1 times

Stiflersammy 1 year ago

Accident can happen if you don't educate. I will go with A since the best way to share is by creating groups the need those confidential document. e.g maybe for Finance, there whould be a finance group and so on.

upvoted 1 times

Jane1234YIP 1 year, 1 month ago

Selected Answer: A

A is correct

Option A involves creating groups based on user roles or departments and then educating users on how to share with those specific groups instead of sharing with "anyone in this group with this link can view." By using groups, users can share items with relevant teams or individuals more easily and reduce the risk of accidental oversharing to the entire organization.

upvoted 2 times

[Removed] 1 year, 1 month ago

Selected Answer: A

the question said "users" meaning the entire organization ...not paying attention to only those who handle sensitive information... C is wrong because it only addresses users who handle sensitive info...what about the rest of the users? they can go ahead and overshare?

upvoted 2 times

danaracena 1 year, 1 month ago

Also answered C. But the key in the question es "PREVENT ACCIDENTALLY SHARING". If you educate, still youre not preventing accidents. The only option that furfill that requi
rement is B.

upvoted 1 times

[Removed] 1 year, 2 months ago

Correct answer is A... Users will now be sharing appropriately, and on top of that they'll be educated

upvoted 1 times

gordonchen8998 1 year, 3 months ago

Selected Answer: C

use trust rules to manage Drive Sharing (https://apps.google.com/supportwidget/articlehome?hl=en&article_url=https%3A%2F%2Fsupport.google.com%2Fa%2Fanswer%2F10621317%3Fhl%3Den&assistant_id=generic-unu&product_context=10621317&product_name=UnuFlow&trigger_context=a) and use primary target audiences to avoid users for accidentery oversharing all users with the link. ()

upvoted 1 times

jaxclain 1 year, 9 months ago

Selected Answer: C

Whoever is elaborating the questions, is not good lol
I will have to say C because is the only option that make sense of the other 3...

upvoted 4 times

RAZKZ 1 year, 9 months ago

B- Does not help users share more appropriately.
C - Does not prevent them from oversharing.

Correct me if i'm wrong, some of these questions are sending me, I don't see an actual correct answer to the question here.

upvoted 2 times

Eagles215Philly 1 year ago

B Does help users to share more apporpriately. They will need to instead of giving the whole org access, they will have to give individuals or groups access. It reduces oversharing as well.

upvoted 1 times

RAZKZ 1 year, 9 months ago

Why does the question say "prevent" oversharing, C does not prevent them, it reduces the chance of it happening...

upvoted 1 times

Willem_M 1 year, 8 months ago

It says "prevent ACCIDENTAL oversharing" so I think they mean, if the default is not "share with everyone" and you still go to find the option to share with the entire organisation, it is not accidental? So C would be good enough I think.

upvoted 2 times

Eagles215Philly 1 year ago

I believe though diasbling sharing to the whole org would in fact make people think who they need to give access to. Hence I think B would do the job.

upvoted 1 times

Question #18 *Topic 1*

You are a Workspace Administrator with a mix of Business Starter and Standard Licenses for your users. A Business Starter User in your domain mentions that they are running out of Drive Storage Quota. Without deleting data from Drive, what two actions can you take to alleviate the quota concerns for this user? (Choose two.)

A. Add other users as “Editors” on the Drive object, thus spreading the storage quota debt between all of them.

B. Manually export and back up the data locally, and delete the affected files from Drive to alleviate the debt.

C. Make another user the “Owner” of the Drive objects, thus transferring the storage quota debt to them.

D. Perform an API query for large storage drive objects, and delete them, thus alleviating the quota debt.

E. Move the affected items to a Shared Drive. Shared Drives transfer ownership of the drive item to the domain itself, which alleviates the quota debt from that user.

Suggested Answer: *DE*

Community vote distribution

CE (82%) Other

jitu028 Highly Voted 1 year, 9 months ago

Selected Answer: CE

Correct answer - CE

upvoted 7 times

Diani 1 year, 8 months ago

Why E? Business Starter hasn't have Shared Drive

upvoted 1 times

userX100 1 year, 5 months ago

A starter user cannot create shared drives but he can participate in them

upvoted 1 times

Dante_Student Most Recent 8 months, 1 week ago

Selected Answer: CE

C and E

upvoted 1 times

virat_kohli 10 months, 1 week ago

Selected Answer: CE

C. Make another user the “Owner” of the Drive objects, thus transferring the storage quota debt to them.
E. Move the affected items to a Shared Drive. Shared Drives transfer ownership of the drive item to the domain itself, which alleviates the quota debt from that user.

upvoted 1 times

jcloud965 10 months, 3 weeks ago

Selected Answer: CE

CE but with new Storage pool, it should related with storage rules

upvoted 1 times

amministrazione 11 months, 3 weeks ago

C. Make another user the “Owner” of the Drive objects, thus transferring the storage quota debt to them.
E. Move the affected items to a Shared Drive. Shared Drives transfer ownership of the drive item to the domain itself, which alleviates the quota debt from that user.

upvoted 1 times

Gomesallef 11 months, 3 weeks ago

Selected Answer: CE

faria muito sentido, migrar os dados de uma conta para outra com drive "ilimitado". para balanciamento.

upvoted 1 times

Steventjie 1 year ago

Haha! Without deleting data from Drive, how do you achieve this?
>Delete data from Drive
upvoted 2 times

baha2 1 year, 3 months ago
Selected Answer: CE
Without deleting data from Drive
upvoted 2 times

Bardapapa 1 year, 3 months ago
Selected Answer: DE
C is not correct as it's not a "serious" solution -
upvoted 2 times

Nico282 9 months ago
Cannot be D, the question stated "without deleting"
upvoted 1 times

userX100 1 year, 5 months ago
Selected Answer: CE
C and E are correct
upvoted 1 times

raquint 1 year, 8 months ago
Selected Answer: BC
E is not because of permissions in Drive. Changing editors won't change storage.
upvoted 2 times

Diani 1 year, 7 months ago
The B can't be because it says "Without deleting data from the drive"
upvoted 2 times

Moss2011 1 year, 8 months ago
I think is B and C because a Business Starter only have "viewer" option to a Share Drive
upvoted 2 times

raquint 1 year, 8 months ago
This is 100% correct. Starter users cannot use Shared Drive. Only as viewers
upvoted 1 times

Mosie23 1 year, 3 months ago
However, if a file in a shared drive is shared with them directly, then they may also be allowed to comment or edit the file.
upvoted 1 times

jaxclain 1 year, 9 months ago
Selected Answer: CE
I agree as well C and E. But there is something wrong about C, it doesn't specify the license of the new owner but is a tipical Google question (they are really bad generating these questions lol).
upvoted 3 times

Willem_M 1 year, 9 months ago
Selected Answer: CE
Only answers without deletion of data
upvoted 1 times

jamesitexpert 1 year, 9 months ago
B Starter users only have Viewer privileges tho
https://support.google.com/a/answer/7337469?hl=en#:~:text=These%20users%20can%20be%20added%20as%20members%20of%20shared%20drives%2C%20but%20only%20with%2
upvoted 2 times

Question #19 *Topic 1*

Your organization is preparing to deploy Workspace and will continue using your company's existing identity provider for authentication and single sign-on (SSO). In order to migrate data from an external system, you were required to provision each user's account in advance. Your IT team and select users (~5% of the organization) have been using Workspace for configuration and testing purposes. The remainder of the organization can technically access their accounts now, but the IT team wants to block their access until the migrations are complete. What should your organization do?

A. Remove Google Workspace license to prevent users from accessing their accounts now.

B. Suspend users that the organization does not wish to have access.

C. Add the users to the OU with all services disabled.

D. Use Context-Aware Access to simultaneously block access to all services for all users and allow access to all services for the allowed users.

Suggested Answer: *B*

Community vote distribution

virat_kohli 10 months, 1 week ago

Selected Answer: D

D. Use Context-Aware Access to simultaneously block access to all services for all users and allow access to all services for the allowed users.

upvoted 1 times

Gomesallef 10 months, 3 weeks ago

Selected Answer: D

Correct answer - D

O restante da organização pode tecnicamente acessar suas contas agora, mas a equipe de TI deseja bloquear o acesso até que as migrações sejam concluídas. Como a equipe de TI deseja bloquear outros usuários e a TI está usando o Workspace para fins de configuração e teste, D está correto.

upvoted 3 times

amministrazione 11 months, 3 weeks ago

D. Use Context-Aware Access to simultaneously block access to all services for all users and allow access to all services for the allowed users.

upvoted 1 times

topnode2023 1 year ago

Selected Answer: D

"Depending on what you're migrating, you need to turn on the relevant service (Gmail for email, Directory for contacts, and Google Calendar for calendar events)."

- https://support.google.com/a/answer/9158145?hl=en

upvoted 2 times

Stiflersammy 1 year ago

Selected Answer: D

The remainder of the organization can technically access their accounts now, but the IT team wants to block their access until the migrations are complete. Since the IT team wants to block other users and IT are using Workspace for configuration and testing purposes D is correct.

upvoted 3 times

Stiflersammy 1 year ago

The remainder of the organization can technically access their accounts now, but the IT team wants to block their access until the migrations are complete. Since the IT team wants to block other users and IT are using Workspace for configuration and testing purposes D is correct.

upvoted 1 times

[Removed] 1 year, 1 month ago

Selected Answer: C
suspending is not necessarry given the circumstance
upvoted 2 times

jdosh 1 year, 3 months ago
Selected Answer: D
D is correct, you cannot migrate to suspended accounts or accounts with disabled services.
upvoted 2 times

Bardapapa 1 year, 3 months ago
Selected Answer: B
B is the correct option
upvoted 1 times

gastonMM 1 year, 5 months ago
Selected Answer: C
test performed: user with disabled services can receive migrated emails with DMS
upvoted 1 times

userX100 1 year, 5 months ago
Selected Answer: D
"In order to migrate data from an external system, you were required to provision each user's account in advance."

A,B,C are not correct because you can't migrate without a license, to a suspended account or with services disabled.

THE CORRECT OPTION IS- D
upvoted 2 times

pgwagopo 1 year, 7 months ago
Selected Answer: D
Vote for D
upvoted 1 times

Rafaelbsa 1 year, 7 months ago
Como os dados precisarem ser migrados, as contas de usuário não podem ser desativadas nem suspensas. Sendo assim não é possível desativar os serviços, por esse motivo com certeza a resposta correta é D.
upvoted 2 times

RAZKZ 1 year, 9 months ago
Selected Answer: C
Definitely C, presented in deployment course from Google for GWS Admin.
upvoted 2 times

jaxclain 1 year, 9 months ago
Selected Answer: C
You don't need to complicate things using Context-aware Access just for this lol, context aware access purpose is somethig totally different, they just want to prevent users from using the services until the migration is done, simply create an OU, add them to it, disable the services and thats it.
upvoted 4 times

jaxclain 1 year, 8 months ago
I have reviewed this question more and just realized that suspended accounts cannot be migrated, both source and destination needs to be active, on this case the migration is external so the destination GW acc needs to be active... https://support.google.com/workspacemigrate/answer/9991417?hl=en#:~:text=Both%20source%20and%20target%20Google,accounts%20can't%20be%20migrated.

So... I could not find anywhere what happens if Gmail is disabled, not sure if the IMAP access will be disabled as well so I assume it will be similar to a suspended account... meaning the correct answer is D?? context aware access?? lol wow I am lost here... if someone can confirm if IMAP access is still available even if Gmail is disabled?
upvoted 2 times

jdosh 1 year, 2 months ago
you're correct it's supposed to be D. you cannot migrate to suspended and disabled service users.
upvoted 1 times

Exam__ 1 year, 9 months ago

Selected Answer: C

Correct answer - C

upvoted 1 times

AmirSBC 1 year, 9 months ago

Selected Answer: B

If the services are disabled, then also data migration for that service would not be possible for the user, So C is not correct

upvoted 3 times

Question #20 *Topic 1*

Your company has acquired a new company in Japan and wants to add all employees of the acquisition to your existing Google Workspace domain. The new company will retain its original domain for email addresses and, due to the very sensitive nature of its work, the new employees should not be visible in the global directory. However, they should be visible within each company's separate directory. What should you do to meet these requirements?

A. Create a new Google Workspace domain isolated from the existing one, and create users in the new domain instead.

B. Under Directory Settings > Contact sharing, disable the contact sharing option and wait for 24 hours to allow the settings to propagate before creating the new employee accounts.

C. Redesign your OU organization to have 2 child OUs for each company directly under the root. In Directory Settings > Visibility Settings, define custom directories for each company, and set up Visibility according to the OU.

D. Create one dynamic group for each company based on a custom attribute defining the company. In Directory Settings > Visibility Settings, define custom directories for each company, and set up Visibility according to the dynamic group.

Suggested Answer: *A*

Community vote distribution

C (100%)

jaxclain Highly Voted 1 year, 9 months ago

Selected Answer: C

C is correct :)

upvoted 6 times

virat_kohli Most Recent 10 months, 1 week ago

Selected Answer: C

C. Redesign your OU organization to have 2 child OUs for each company directly under the root. In Directory Settings > Visibility Settings, define custom directories for each company, and set up Visibility according to the OU.

upvoted 1 times

jcloud965 10 months, 2 weeks ago

Selected Answer: C

C is correct

Directory Visibility Setting is OU based. Custom Directory is Group based.

upvoted 1 times

Gomesallef 10 months, 3 weeks ago

Selected Answer: C

Correct Answer - C

upvoted 1 times

amministrazione 11 months, 3 weeks ago

C. Redesign your OU organization to have 2 child OUs for each company directly under the root. In Directory Settings > Visibility Settings, define custom directories for each company, and set up Visibility according to the OU.

upvoted 1 times

Gomesallef 11 months, 3 weeks ago

Selected Answer: C

Correct Answer - C

https://support.google.com/a/answer/7566446?hl=en&ref_topic=9832541

upvoted 2 times

Steventjie 1 year ago

Lmao!

"wants to add all employees of the acquisition to your existing Google Workspace domain"

>Create a new Google Workspace domain isolated from the existing one

upvoted 1 times

[Removed] 1 year, 1 month ago

Selected Answer: C

C is correct for sure

upvoted 1 times

userX100 1 year, 1 month ago

Selected Answer: C

C is correct

upvoted 1 times

[Removed] 1 year, 2 months ago

D is correct

upvoted 1 times

RAZKZ 1 year, 9 months ago

How does C help them retain the original domain for email access?

upvoted 2 times

jaxclain 1 year, 8 months ago

Separating teams by Organizational Units is the best way to manage different Organizations in huge companies, like for example Google, for sure has different OU structures for YouTube, Google Workspace, Google Cloud, etc, I did work for Google Workspace and I never saw any contact from YouTube but I know YouTube is part of the Google (Google Workspace) account :)

upvoted 5 times

pid 1 year, 6 months ago

C is the only one that makes sense, although it does not cover the part in the answer about adding email alias for new company so that users can retain email access.

upvoted 2 times

HEA22 1 year, 9 months ago

Selected Answer: C

C seems the logic answer. But the question of all this exam are very badly set imo...

upvoted 3 times

Sav94 1 year, 9 months ago

C - answer other questions :)

upvoted 3 times

impearl 1 year, 9 months ago

Correct Answer - C

https://support.google.com/a/answer/7566446?hl=en&ref_topic=9832541

upvoted 4 times

Question #21 *Topic 1*

You are in the middle of migrating email from on-premises Microsoft Exchange to Google Workspace. Users that you have already migrated are complaining of messages from internal users going into spam folders. What should you do to ensure that internal messages do not go into Gmail spam while blocking spoofing attempts?

A. Train users to click on Not Spam button for emails.

B. Add all users of your domain to an approved sender list.

C. Force TLS for your domain.

D. Ensure that your inbound gateway is configured with all of your Exchange server IP addresses.

Suggested Answer: *B*

Community vote distribution

D (89%) 11%

jaxclain Highly Voted 1 year, 9 months ago

Selected Answer: D

This is very tricky because D is also correct, I have done mgirations from On Premises before and you can switch the MX records poitining to Google, configure the Inbound Gateway to make sure emails are not mark as spam and that's it but also B would work.

I will vote for D because I saw the Deployment Videos from Google and as best practice to migrate from On Premises, they do recommend to do it as I mentioned so I assume they are refering this question to that part of the Google guide. Also the question is not clear if the MX records are poiting to Google, I would assume they are so yeah, I would go for D lol

upvoted 5 times

Nico282 Most Recent 8 months, 4 weeks ago

Selected Answer: D

I think "while blocking spoofing attempts" excludes option B

upvoted 1 times

virat_kohli 10 months, 1 week ago

Selected Answer: D

D. Ensure that your inbound gateway is configured with all of your Exchange server IP addresses.

upvoted 1 times

amministrazione 11 months, 3 weeks ago

D. Ensure that your inbound gateway is configured with all of your Exchange server IP addresses.

upvoted 1 times

[Removed] 1 year, 1 month ago

Selected Answer: D

In a migration process it is important to have the Exchange IP configured to avoid this behavior

upvoted 2 times

NoName2546 1 year, 2 months ago

Selected Answer: D

Confirmed Option D:
https://support.google.com/a/answer/9228551#legacy-as-primary

After migrating from exchange, you configure a forwarding of migrated mailboxes to Workspace, and you need to configure inbound mail gateway to allow the high volume traffic coming from the exchange.

upvoted 2 times

jdosh 1 year, 3 months ago

Selected Answer: D

I just completed a project like this a few months ago. D is the correct answer.

upvoted 1 times

pid 1 year, 6 months ago

Selected Answer: D

Definitely D;

. If you are forwarding mail to Gmail from another mail system (perhaps you are in the process of migrating users onto Google Workspace) you should not add your legacy server's IP address(es) to the email whitelist. Add the address(es) to the inbound gateway section instead.

upvoted 2 times

Moss2011 1 year, 8 months ago

Selected Answer: D

In a migration process it is important to have the Exchange IP configured to avoid this behavior

upvoted 1 times

RAZKZ 1 year, 9 months ago

Selected Answer: D

Going with D on this one:
https://support.google.com/a/answer/60730?hl=en
Not directly mentioned in the link above, but mentioned in an official google course.

upvoted 1 times

AsakuraYoh 1 year, 9 months ago

D is the correct Answer!

upvoted 2 times

RAZKZ 1 year, 9 months ago

Isn't this D?
https://support.google.com/a/answer/60730?hl=en

upvoted 3 times

jitu028 1 year, 9 months ago

correct answer - B
https://support.google.com/a/answer/60752?hl=en#:~:text=Approved%20senders%20list%E2%80%94,settings%20in%20Google%20Workspace.

upvoted 2 times

jitu028 1 year, 9 months ago

Selected Answer: B

Correct answer - B
Approved senders list—Approved senders are trusted users that send email to your organization. Create an address list of approved senders so messages from these users bypass Gmail's spam filters, and recipients can decide whether they are spam or not. Create the list with individual email addresses, or by adding an entire domain.

upvoted 2 times

Question #22 *Topic 1*

A user is reporting that after they sign in to Gmail, their labels are not loading and buttons are not responsive. What action should you take to troubleshoot this issue with the user?

A. Collect full message headers for examination.

B. Check whether the issue occurs when the user authenticates on a different device or a new incognito window.

C. Check whether a ping test to service.gmail.com (pop.gmail.com or imap.gmail.com) is successful.

D. Check whether traceroute to service.gmail.com (pop.gmail.com or imap.gmail.com) is successful.

Suggested Answer: *A*

Community vote distribution

B (100%)

virat_kohli 10 months, 1 week ago

Selected Answer: B

B. Check whether the issue occurs when the user authenticates on a different device or a new incognito window.

upvoted 1 times

Gomesallef 10 months, 3 weeks ago

Selected Answer: B

B. Check whether the issue occurs when the user authenticates on a different device or a new incognito window.

upvoted 1 times

amministrazione 11 months, 3 weeks ago

B. Check whether the issue occurs when the user authenticates on a different device or a new incognito window.

upvoted 1 times

BearPop 1 year, 1 month ago

Selected Answer: B

Definately B

upvoted 1 times

[Removed] 1 year, 2 months ago

B please

upvoted 1 times

jdosh 1 year, 3 months ago

Selected Answer: B

I'm regretting paying contributors access for this one, so many wrong answers.

upvoted 3 times

d7d508d 11 months, 1 week ago

me too

upvoted 1 times

baha2 1 year, 3 months ago

Selected Answer: B

Option B correct

upvoted 1 times

denHuw 1 year, 4 months ago

Selected Answer: B

The answer is B. Collecting email headers is completely pointless, because the problem is in the interface, not in the emails.

upvoted 1 times

jaxclain 1 year, 9 months ago

Selected Answer: B

Option B seems correct, all other options make no sense, no need message header for this (A), or troubleshoot the network (C and D), you can leave that at the end in case nothing else works so obviously is the network, nothing to do with the GW service.

upvoted 3 times

Exam__ 1 year, 9 months ago

Selected Answer: B

correct answer - B

upvoted 2 times

jitu028 1 year, 9 months ago

Selected Answer: B

correct answer - B

upvoted 2 times

Question #23 *Topic 1*

A retail company has high employee turnover due to the cyclical nature in the consumer space. The increase in leaked confidential content has created the need for a specific administrative role to monitor ongoing employee security investigations. What step should you take to increase the visibility of such investigations?

A. Assign the ‘Services Admin’ role to an administrator with ‘Super Admin’ privileges.

B. Create a ‘Custom Role’ and add all the Google Vault privileges for a new administrator.

C. Validate that the new administrator has access to Google Vault.

D. Create a ‘Custom Role’ and add the ability to manage Google Vault matters, holds, searches, and exports.

Suggested Answer: *D*

Community vote distribution

D (93%) 7%

Gomesallef 10 months, 3 weeks ago

Selected Answer: D

D. Create a ‘Custom Role’ and add the ability to manage Google Vault matters, holds, searches, and exports.

upvoted 1 times

amministrazione 11 months, 3 weeks ago

D. Create a ‘Custom Role’ and add the ability to manage Google Vault matters, holds, searches, and exports.

upvoted 1 times

BearPop 1 year, 1 month ago

Selected Answer: D

Definately D

upvoted 2 times

jaxclain 1 year, 9 months ago

Selected Answer: D

I would go for D because B is adding all Google Vault privileges include manage retentions and audits, the most important here is audits because this is how the Super Admin will audit what the Vault Admin is doing, still there is not an option to delete Audits but he will be able to see other admins vault audits, as a best practice for Google, I believe assigning the Custom Role with just the enough privileges will be ok, here you can view the Vault Privileges: https://support.google.com/vault/answer/2799699

upvoted 4 times

testseb 1 year, 9 months ago

Selected Answer: D

you don't want the new "admin" to mess with your Retention policies. So only 4 rights are enough!

upvoted 3 times

impearl 1 year, 9 months ago

Selected Answer: D

I think that just add to Google Vault metters, holds, searches, exports. You do not have to add all the Google Vault Previleages.

upvoted 4 times

jitu028 1 year, 9 months ago

Selected Answer: B

correct answer - B, as it is asking to create new admin role as well, compared to D which is only creating the new role but not assigning to default super admin which already has all the required privileges.

upvoted 1 times

RAZKZ 1 year, 9 months ago

Aren't they asking to create a new administrative role? assigning it to a new admin seems implicit.

So many of these questions are vague imo

upvoted 1 times

Question #24 *Topic 1*

A subset of users from the finance and human resources (HR) teams need to share documents with an external vendor. However, external content sharing is prohibited for the entire finance team. What would be the most secure method to enable external sharing for this set of users?

A. Download and attach the documents to a Gmail message, and send them to the external vendor.

B. Move all users from the finance org unit to the HR org unit.

C. Enable 'Visitor Sharing' for the entire finance org unit.

D. Create a group with the finance and HR users who need to share externally.

Suggested Answer: *D*

Community vote distribution

D (100%)

virat_kohli 10 months, 1 week ago

Selected Answer: D

D. Create a group with the finance and HR users who need to share externally.

upvoted 1 times

Gomesallef 10 months, 3 weeks ago

Selected Answer: D

Correct answer - D

upvoted 1 times

amministrazione 11 months, 3 weeks ago

D. Create a group with the finance and HR users who need to share externally.

upvoted 1 times

jaxclain 1 year, 9 months ago

Selected Answer: D

D seems correct to me

upvoted 2 times

jitu028 1 year, 9 months ago

Selected Answer: D

Correct answer - D

upvoted 3 times

Question #25 *Topic 1*

As the newly hired Admin in charge of Google Workspace, you learn that the organization has been using Google Workspace for months and has configured several security rules for accessing Google Drive. A week after you start your role, users start to complain that they cannot access Google Drive anymore from one satellite office and that they receive an error message that “a company policy is blocking access to this app.” The users have no issue with Gmail or Google Calendar. While investigating, you learn that both this office's Internet Service Provider (ISP) and the global IP address when accessing the internet were changed over the weekend. What is the most logical reason for this issue?

A. An access level was defined based on the IP range and applied to Google Drive via Context-Aware Access.

B. Under Drive and Docs > Sharing Settings, the “Whitelisted domains” list needs to be updated to add the new ISP domain.

C. The Network Mask defined in Security > Settings > SSO with 3rd Party IdPs should be updated to reflect the new IP range.

D. You need to raise a ticket to Google Cloud Support to have your new IP ranges registered for Drive API access.

Suggested Answer: *A*

Community vote distribution

A (100%)

virat_kohli 10 months, 1 week ago

Selected Answer: A

A. An access level was defined based on the IP range and applied to Google Drive via Context-Aware Access.

upvoted 1 times

amministrazione 11 months, 3 weeks ago

A. An access level was defined based on the IP range and applied to Google Drive via Context-Aware Access.

upvoted 2 times

jaxclain 1 year, 9 months ago

Selected Answer: A

A easy :)

upvoted 1 times

RAZKZ 1 year, 9 months ago

Selected Answer: A

IMO it's A:
https://support.google.com/a/answer/9262032?hl=en#zippy=%2Cdefine-access-levelsadvanced-mode%2Cdefine-access-levelsbasic-mode

upvoted 2 times

jitu028 1 year, 9 months ago

Selected Answer: A

correct answer - A

upvoted 1 times

Question #26 *Topic 1*

An end user informs you that they are having issues receiving mail from a specific sender that is external to your organization. You believe the issue may be caused by the external entity's SPF record being incorrectly configured. Which troubleshooting step allows you to examine the full message headers for the offending message to determine why the messages are not being delivered?

A. Use the Postmaster Tools API to pull the message headers.

B. Use the Email Log Search to directly review the message headers.

C. Use the Security Investigation Tool to review the message headers.

D. Perform an SPF record check on the domain to determine whether their SPF record is valid.

Suggested Answer: *D*

Community vote distribution

C (65%) B (29%) 6%

qtDirk 4 months ago

C - in the email log search you only get Message details and recipient details. On the investigation tool you get the Raw Headers.

upvoted 1 times

Nico282 9 months ago

Selected Answer: C

The Security investigation Tool shows the full message headers, including SPF, DKIM and DMARC. Checked on the Admin console.

upvoted 1 times

virat_kohli 10 months, 1 week ago

Selected Answer: C

C. Use the Security Investigation Tool to review the message headers.

upvoted 1 times

jcloud965 10 months, 3 weeks ago

Selected Answer: C

Email Log Search doesn't include the headers.

The investigation tool allows you to have a look at an entire message including headers.

Correct answer is C.

upvoted 1 times

amministrazione 11 months, 3 weeks ago

B. Use the Email Log Search to directly review the message headers.

upvoted 1 times

jcloud965 10 months, 3 weeks ago

Email Log Search doesn't include the headers

upvoted 1 times

[Removed] 1 year, 1 month ago

Selected Answer: B

Correct answer is B

https://support.google.com/a/answer/7513679?hl=en

upvoted 3 times

danaracena 1 year, 1 month ago

Selected Answer: D

Is D ... dont get me wrong. That is not the solution. But the question states that as Admin you are already thinking that the problem was con SPF ... In that line, the most obvious first step (if we are thinking that) is to check on SPF

upvoted 1 times

azsamtuk 11 months, 1 week ago

The question states exactly: "Which troubleshooting step allows you to examine the full message headers..."

upvoted 2 times

jaxclain 1 year, 9 months ago

Selected Answer: C

Also agree with C, you can view the Message Header, the other 3 options will not show the Message Header and that's the priority on this question. Also Google Vault but is not on this list.

upvoted 1 times

[Removed] 1 year, 1 month ago

email log search shows the header

upvoted 1 times

RAZKZ 1 year, 9 months ago

Can someone explain why it's not D?

Also, do we even know it reached our servers?

upvoted 3 times

jaxclain 1 year, 9 months ago

lol the question says: "Which troubleshooting step allows you to examine the full message headers for the offending message to determine why the messages are not being delivered?".

So yes, the only viable option is C, I was a GW Admin / Deployment specialist for almost 7-8 years so I am 100% sure the Investigation tool will show the message header lol

upvoted 3 times

certificationDJJ 1 year, 9 months ago

Selected Answer: C

Reason: the log search will only see the disposition of the email (who sent it, received it, reason for refusing delivery, IP. It does not show the message header.

upvoted 3 times

RJRF503 1 year, 9 months ago

Selected Answer: C

The question says to review Full message header. Email log search doesn't allow you to see full message header. Security tool does this https://support.google.com/a/answer/9300435?hl=en#zippy=%2Cstep-view-the-email-message-and-take-action%2Cstep-provide-justification-to-view-messages%2Cstep-get-started-with-your-investigation

upvoted 4 times

jitu028 1 year, 9 months ago

Selected Answer: B

Correct answer is B

https://support.google.com/a/answer/7513679?hl=en

upvoted 2 times

certificationDJJ 1 year, 9 months ago

Wrong!

Correct is the alternative C:

Reason: the log search will only see the disposition of the email (who sent it, received it, reason for refusing delivery, IP. It does not show the message header.

upvoted 2 times

RAZKZ 1 year, 9 months ago

Aren't we not even receiving the mail? how would you search for it on our side in the admin console?

upvoted 3 times

Question #27 *Topic 1*

You have been asked to support an investigation that your litigation team is conducting. The current default retention policy for mail is 180 days, and there are no custom mail retention policies in place. The litigation team has identified a user who is central to the investigation, and they want to investigate the mail data related to this user without the user's awareness. What two actions should you take? (Choose two.)

A. Move the user to their own Organization Unit, and set a custom retention policy.

B. Create a hold on the user's mailbox in Google Vault.

C. Reset the user's password, and share the new password with the litigation team.

D. Copy the user's data to a secondary account.

E. Create a matter using Google Vault, and share the matter with the litigation team members.

Suggested Answer: *BE*

Community vote distribution

BE (100%)

virat_kohli 10 months, 1 week ago

Selected Answer: BE

B. Create a hold on the user's mailbox in Google Vault.

E. Create a matter using Google Vault, and share the matter with the litigation team members.

upvoted 1 times

amministrazione 11 months, 3 weeks ago

B. Create a hold on the user's mailbox in Google Vault.

E. Create a matter using Google Vault, and share the matter with the litigation team members.

upvoted 1 times

BearPop 1 year, 1 month ago

Selected Answer: BE

BE are correct

upvoted 1 times

jaxclain 1 year, 9 months ago

Selected Answer: BE

100% B and E are correct, holds will take over any retention policy so first, create the hold on the users mailbox then create the matter, do the search of the user data and share it with the litigation team.

upvoted 4 times

jitu028 1 year, 9 months ago

Selected Answer: BE

Correct answer - BE

upvoted 3 times

Question #28 *Topic 1*

A recent legal investigation requires all emails and Google Drive documents from a specific user to be retrieved. As the administrator, how can you fulfill the legal team's request?

A. Use Security Investigation Tool to Search Google Drive events for all of the user's documents, and use Google Admin > Reports > Email Log Search to find their emails.

B. Search Google Drive for all of the user's documents, and ask them to forward all of their emails.

C. Use the Gmail API and Google Drive API to automatically collect and export data.

D. Utilize Google Vault to hold, search, and export data of interest.

Suggested Answer: *A*

Community vote distribution

D (100%)

jaxclain Highly Voted 1 year, 9 months ago

Selected Answer: D

D is the correct answer for sure, just keep in mind that Vault will not export folders / labels, just raw data so for emails, you need to look at the header to see if the email belongs to a label or if it was sent, received, deleted, etc... This is why Vault is not recommended for doing Backups but analizing the 4 options here, A will not work, B is too exausting, C will work but you will need a 3rd party app or something like Google Workspace Migrate but that service is only for Enterprise companies so the only option left is D lol

upvoted 5 times

virat_kohli Most Recent 10 months, 1 week ago

Selected Answer: D

D. Utilize Google Vault to hold, search, and export data of interest.

upvoted 1 times

amministrazione 11 months, 3 weeks ago

D. Utilize Google Vault to hold, search, and export data of interest.

upvoted 1 times

danaracena 1 year, 1 month ago

Selected Answer: D

I also chose D. But checked on my console and A is also possible.

Yet i cannot understand why A would be a better option for the case than D ..

upvoted 1 times

jdosh 1 year, 3 months ago

Selected Answer: D

no brainer

upvoted 2 times

hehe_24 1 year, 9 months ago

Selected Answer: D

D is the one guys

upvoted 3 times

AsakuraYoh 1 year, 9 months ago

Selected Answer: D

D is the correct answer

upvoted 3 times

jitu028 1 year, 9 months ago

Selected Answer: D

correct answer - D

upvoted 4 times

Question #29 *Topic 1*

What steps does an administrator need to take to enforce TLS with a particular domain?

A. Enable email safety features with the receiving domain.

B. Set up secure transport compliance with the receiving domain.

C. Configure an alternate secure route with the receiving domain.

D. Set up DKIM authentication with the receiving domain.

Suggested Answer: *B*

Community vote distribution

B (100%)

virat_kohli 10 months, 1 week ago

Selected Answer: B

B. Set up secure transport compliance with the receiving domain.

upvoted 1 times

Gomesallef 11 months, 2 weeks ago

Selected Answer: B

B correct. Set up secure transport compliance with the receiving domain.

upvoted 2 times

amministrazione 11 months, 3 weeks ago

B. Set up secure transport compliance with the receiving domain.

upvoted 1 times

BearPop 1 year, 1 month ago

Selected Answer: B

B is correct

upvoted 1 times

jaxclain 1 year, 8 months ago

Selected Answer: B

B is correct

upvoted 2 times

jitu028 1 year, 9 months ago

Selected Answer: B

Correct answer - B

https://support.google.com/a/answer/2520500?hl=en#:~:text=Add%C2%A0the%20Secure%20transport%20(TLS)%20compliance%C2%A0setting%C2%A0to%20always%20use%20TLS

upvoted 4 times

Question #30 *Topic 1*

Your company's Google Workspace primary domain is "mycompany.com," and it has acquired a startup that is using another cloud provider with a domain named "mystartup.com." You plan to add all employees from the startup to your Google Workspace domain while preserving their current mail addresses. The startup CEO's email address is andrea@mystartup.com, which also matches your company CEO's email address as andrea@mycompany.com, even though they are different people. Each must keep the usage of their email. In addition, your manager asked to have all existing security policies applied for the new employees without any duplication. What should you do to implement the migration?

A. Create a secondary domain, mystartup.com, within your current Google Workspace domain, set up necessary DNS records, and create all startup employees with the secondary domain as their primary email addresses.

B. Create an alias domain, mystartup.com, in your existing Google Workspace domain, set up necessary DNS records, and create all startup employees with the alias domain as their primary email addresses.

C. Create a new Google Workspace domain with "mystartup.com," and create a trust between both domains for reusing the same security policies and sharing employee information within the companies.

D. Create the startup employees in the "mycompany.com' domain, and add a number at the end of the user name whenever there is a conflict. In Gmail > Routing, define a specific route for the OU that targets the startup employees, which will modify the email address domain to "mystartup.com," and remove any numbers previously added. In addition, confirm that the SPF and DKIM records are properly set.

Suggested Answer: *D*

Community vote distribution

A (100%)

jaxclain Highly Voted 1 year, 9 months ago

Selected Answer: A

A is the only answer that makes sense.

upvoted 7 times

virat_kohli Most Recent 10 months, 1 week ago

Selected Answer: A

A. Create a secondary domain, mystartup.com, within your current Google Workspace domain, set up necessary DNS records, and create all startup employees with the secondary domain as their primary email addresses.

upvoted 1 times

Gomesallef 11 months, 2 weeks ago

Selected Answer: A

Letter A - Secondary domain.

upvoted 1 times

amministrazione 11 months, 3 weeks ago

A. Create a secondary domain, mystartup.com, within your current Google Workspace domain, set up necessary DNS records, and create all startup employees with the secondary domain as their primary email addresses.

upvoted 1 times

BearPop 1 year, 1 month ago

Selected Answer: A

A is the one!

upvoted 1 times

jdosh 1 year, 3 months ago

Selected Answer: A

easy A

upvoted 2 times

pid 1 year, 6 months ago

You can easily do this with A

upvoted 2 times

jitu028 1 year, 9 months ago

Selected Answer: A

correct answer - A

upvoted 3 times

RAZKZ 1 year, 9 months ago

It's asked both have the same security policy without duplication, can we do that if A?

upvoted 1 times

jaxclain 1 year, 9 months ago

@RAZKZ, what is wrong with A? lol having a secondary domain, creating the incoming users with that domain, you can add them to a sub OU, also the policies applied at the OU level will apply to those incoming users, the other options B, C and D makes no sense so you need to get used to Google exams... as a tip if this is your first exam, just look for the most logical answer, discard the less logical or the ones that makes no sense, in the end you will always have 2 options lol

I have done many Google exams.. CDL, ACE, PCA twice and next week i will do this exam lol

upvoted 4 times

Mauricio1993 1 year, 3 months ago

you pass ?

upvoted 3 times

Question #31 *Topic 1*

You are in charge of automating and configuring Google Cloud Directory Sync for your organization. Within the config manager, how can you proactively prevent applying widespread deletions within your Workspace environment if your company's LDAP undergoes a substantial modification?

A. Manually run Google Cloud Directory Sync only after performing a simulated sync.

B. Specify the minimum and maximum number of objects to synchronize in each configuration item.

C. Configure the tool to delete users only when run from the config manager.

D. Configure limits for the maximum number of deletions on each synchronization.

Suggested Answer: *B*

Community vote distribution

D (100%)

virat_kohli 10 months, 1 week ago

Selected Answer: D

D. Configure limits for the maximum number of deletions on each synchronization.

upvoted 1 times

Gomesallef 11 months, 2 weeks ago

Selected Answer: D

D. Configure limits for the maximum number of deletions on each synchronization.

https://support.google.com/a/answer/9520714?fl=1

upvoted 1 times

amministrazione 11 months, 3 weeks ago

D. Configure limits for the maximum number of deletions on each synchronization.

upvoted 1 times

BearPop 1 year, 1 month ago

Selected Answer: D

Definately D

upvoted 1 times

baha2 1 year, 3 months ago

Selected Answer: D

Widespread deletions

upvoted 2 times

jaxclain 1 year, 9 months ago

Selected Answer: D

Same I also believe option D is correct because the question also mentions "Widespread deletions" so yes, just limit the maximum number of deletions on each sync.

upvoted 3 times

Exam__ 1 year, 9 months ago

Selected Answer: D

Answer is D

https://support.google.com/a/answer/9520714?fl=1

upvoted 3 times

RJRF503 1 year, 9 months ago

Answer is D

You can use limits with Google Cloud Directory Sync (GCDS) to set the maximum number of deletions permitted on each simulation or synchronization. If it reaches this limit, GCDS stops and does not sync any changes.

https://support.google.com/a/answer/9520714?fl=1

upvoted 2 times

impearl 1 year, 9 months ago

Answer is D

https://support.google.com/a/answer/9520714?fl=1

upvoted 4 times

Question #32 *Topic 1*

Your company recently acquired an organization that was not leveraging Google Workspace. Your company is currently using Google Cloud Directory Sync (GCDS) to sync from an LDAP directory into Google Workspace. You want to deploy a second instance of GCDS and apply the same strategy with the newly acquired organization, which also has its users in an LDAP directory. How should you change your GCDS instance to ensure that the setup is successful? (Choose two.)

A. Provide your current GCDS instance with admin credentials to the recently acquired organization's LDAP directory.

B. Add an LDAP sync rule to your current GCDS instance in order to synchronize new users.

C. Set up exclusion rules to ensure that users synced from the acquired organization's LDAP are not, suspended.

D. Set up an additional instance of GCDS running on another server, and handle the acquired organization's synchronization.

E. Upgrade to the multiple LDAP version of GCDS.

Suggested Answer: *AD*

Community vote distribution

CD (100%)

RJRF503 Highly Voted 1 year, 9 months ago

Selected Answer: CD

Correct answer - C & D

https://support.google.com/a/answer/7177266?hl=en#zippy=%2Ccan-i-sync-gcds-from-multiple-ldap-directories

GCDS can only sync from a single LDAP directory. If you have multiple LDAP directories, it is recommended that you consolidate your LDAP server data into a single directory.

You need to run 2 separate GCDS instances while creating exclusion rules to prevent suspensions/deletions.

upvoted 7 times

Nico282 Most Recent 8 months, 4 weeks ago

Selected Answer: CD

Explanation for the exclusion rule from https://support.google.com/a/answer/7177266 :

Why is my Google Workspace user account being suspended after I run GCDS?

If a Google Workspace user account is suspended after running GCDS, you will receive an error explaining why this happened. In order to avoid repeating the particular error on any subsequent syncs, you can implement one of the following solutions depending on the cause of the problem:

Problem: The user doesn't exist on the LDAP server.

Solution: Since the user doesn't exist on the LDAP server, the customer should set a Google user exclusion rule to prevent GCDS from suspending this user in Google Workspace.

upvoted 1 times

virat_kohli 10 months, 1 week ago

Selected Answer: CD

C. Set up exclusion rules to ensure that users synced from the acquired organization's LDAP are not suspended.

D. Set up an additional instance of GCDS running on another server, and handle the acquired organization's synchronization.

upvoted 1 times

Gomesallef 11 months, 1 week ago

Selected Answer: CD

Resposta correta - C e D https://support.google.com/a/answer/7177266?hl=en#zippy=%2Ccan-i-sync-gcds-from-multiple-ldap-directories O GCDS só pode sincronizar de um único diretório LDAP. Se você tiver vários diretórios LDAP, é recomendável consolidar os dados do servidor LDAP em um único diretório. Você precisa executar duas instâncias separadas do GCDS ao criar regras de exclusão para evitar suspensões/exclusões.

upvoted 1 times

amministrazione 11 months, 3 weeks ago

C. Set up exclusion rules to ensure that users synced from the acquired organization's LDAP are not, suspended.

D. Set up an additional instance of GCDS running on another server, and handle the acquired organization's synchronization.

upvoted 1 times

denHuw 1 year, 4 months ago

Selected Answer: CD

GCDS can only authenticate a single admin, so the answer A is completely wrong.

upvoted 1 times

jaxclain 1 year, 9 months ago

Selected Answer: CD

C and D are correct, first you need to add the exclusion rules on the first GCDS instance to avoid suspensions of newly provisioned users from the second GCDS instance. Then just setup the second GCDS instance in the acquired organization, it will provision and sync those users and those newly provisioned users wont be suspended by the first instance :)

upvoted 3 times

Question #33 *Topic 1*

A user reached out to the IT department about a Google Group that they own: info@company.com. The group is receiving mail, and each message is also delivered directly to the user's Gmail inbox. The user wants to be able to reply to messages directly from Gmail and have them sent on behalf of the group, not their individual account. Currently, their replies come from their individual account. What would you instruct the user to do?

A. Create a new content compliance rule that matches the user's outgoing messages with the group copied, and have it modify the sender to be the group address.

B. Add the group as an email address that can be sent from within Gmail, and verify that the user has access. They can then choose to reply from the group.

C. Add the user's individual account as a delegate to the group's inbox. They can then toggle between the accounts and use the Gmail interface on behalf of the group.

D. Set the group address to be the default sender within the group's posting policies.

Suggested Answer: *C*

Community vote distribution

B (92%) 8%

rune92 10 months ago

Selected Answer: B

B is the right answer

upvoted 1 times

virat_kohli 10 months, 1 week ago

Selected Answer: B

B. Add the group as an email address that can be sent from within Gmail, and verify that the user has access. They can then choose to reply from the group.

upvoted 1 times

Gomesallef 11 months, 2 weeks ago

Selected Answer: B

correct B - funciona da mesma forma que um alias, você adiciona o endereço de e-mail do grupo a "Enviar e-mail como" nas configurações do Gmail, usando a opção "tratar como alias" e está tudo pronto.

upvoted 1 times

amministrazione 11 months, 3 weeks ago

B. Add the group as an email address that can be sent from within Gmail, and verify that the user has access. They can then choose to reply from the group.

upvoted 1 times

BearPop 1 year, 1 month ago

Selected Answer: B

B is the one

upvoted 1 times

[Removed] 1 year, 2 months ago

B is your answer

upvoted 1 times

denHuw 1 year, 4 months ago

Clearly B. As stated in the question, "the user wants to reply from his inbox". Switching between inbox and Groups Interface isn't an option in this case.

upvoted 1 times

jaxclain 1 year, 9 months ago

Selected Answer: B

Option B is correct, it works the same as an Alias, you add the Group email address to the "Send Mail As" from your GW Gmail settings, using the "treat as an alias" option and you are all set.

upvoted 2 times

Exam__ 1 year, 9 months ago

Selected Answer: B

changing answer to B

upvoted 1 times

jitu028 1 year, 9 months ago

changing answer to B

https://support.google.com/googlecloud/answer/10635789?hl=en

upvoted 1 times

RJRF503 1 year, 9 months ago

Selected Answer: B

Correct answer - B

https://support.google.com/mail/answer/22370?hl=en

Configure Send Mail As.

upvoted 4 times

jitu028 1 year, 9 months ago

Selected Answer: D

Correct answer - D

upvoted 1 times

jdosh 1 year, 2 months ago

there's no setting like this so your individual Gmail can reply as the group.

upvoted 1 times

Question #34 *Topic 1*

Your organization recently deployed Google Workspace. Your admin team has been very focused on configuring the core services for your environment, which has left you little time to pay attention to other areas. Your security team has just informed you that many users are leveraging unauthorized add-ons, and they are concerned about data exfiltration. The admin team wants you to cut off all add-ons access to Workspace data immediately and block all future add-ons until further notice. However, they approve of users leveraging their Workspace accounts to sign into third-party sites. What should you do?

A. Modify your Marketplace Settings to block users from installing any app from the Marketplace.

B. Set all API services to “restricted access” and ensure that all connected apps have limited access.

C. Remove all client IDs and scopes from the list of domain-wide delegation API clients.

D. Block each connected app's access.

Suggested Answer: *C*

Community vote distribution

B (72%) C (28%)

05fe736 2 months, 2 weeks ago

Selected Answer: C

"Cut off and block all future add-ons" is different to "restricted / limited access".

upvoted 1 times

virat_kohli 10 months, 1 week ago

Selected Answer: B

B. Set all API services to “restricted access” and ensure that all connected apps have limited access.

upvoted 1 times

Cert1Magic2 10 months, 3 weeks ago

Question says "The admin team wants you to cut off all add-ons access to Workspace data immediately and block all future add-ons until further notice" then why not C, why we will put in restricted access rather than totally cutting it off.

upvoted 2 times

Gomesallef 11 months, 2 weeks ago

Selected Answer: B

B está correto. Ao definir todos os serviços de API como "acesso restrito", você pode limitar efetivamente o acesso que os aplicativos conectados têm aos dados do Google Workspace. Isso ajuda a resolver as preocupações de segurança levantadas pela sua equipe de segurança em relação a complementos não autorizados e possível exfiltração de dados. Você pode revisar e configurar as permissões concedidas a cada aplicativo conectado para garantir que eles tenham acesso limitado apenas aos dados e funcionalidades necessários.

upvoted 1 times

amministrazione 11 months, 3 weeks ago

B. Set all API services to “restricted access” and ensure that all connected apps have limited access.

upvoted 1 times

Jane1234YIP 1 year, 1 month ago

Selected Answer: B

B is correct

By setting all API services to "restricted access," you can effectively limit the access that connected apps have to your Google Workspace data. This helps address the security concerns raised by your security team regarding unauthorized add-ons and potential data exfiltration. You can review and configure the permissions granted to each connected app to ensure they have limited access only to the necessary data and functionality.

upvoted 2 times

juuhcsr1 1 year, 1 month ago

Selected Answer: B

Option C would remove all client IDs and scopes from the list of domain-wide delegation API clients, which would prevent all connected apps from accessing Workspace data. However, this would also prevent users from signing into third-party sites with their

Workspace accounts.
upvoted 2 times

[Removed] 1 year, 2 months ago
D is the answer
upvoted 1 times

jdosh 1 year, 3 months ago
Selected Answer: B
B is the answer because if you don't set the API to restricted then the users will just use new and other add-ons after you do letter c
upvoted 1 times

karl19 1 year, 3 months ago
Selected Answer: B
B. Set all API services to "restricted access" and ensure that all connected apps have limited access.

By setting API services to "restricted access," you can control the access and permissions granted to third-party apps and add-ons. This allows you to review and manage the level of access each app has to Workspace data. Additionally, ensuring that all connected apps have limited access helps minimize the risk of data exfiltration or unauthorized data access.

This approach allows users to continue leveraging their Workspace accounts to sign into third-party sites while maintaining control over the add-ons and their access to Workspace data.
upvoted 4 times

pid 1 year, 6 months ago
Not an answer to this question but there is a new option in settings of Gsuite which will easily satisfy this need - Allow users to access third-party apps that only ask for Google sign-in info
upvoted 3 times

muteto 1 year, 8 months ago
Selected Answer: C
I think the keyword here is "immediately", but want to hear your comments as well?
upvoted 1 times

MC2442 1 year, 8 months ago
Selected Answer: B
This must be B; the limited element ensures the Google Sign-in can still be used and the restriction prevents the add-ons to use company data.
upvoted 1 times

jaxclain 1 year, 8 months ago
Selected Answer: C
I would say C because the option B is not clear, there is an option to block all third party APIs in the Admin Console > APIs section but is not listed here and API services to "restricted access" is not clear because it says that all connected apps have limited access.. In case you need documentation, juti028 already left the link: https://support.google.com/a/answer/162106?hl=en&fl=1#zippy=%2Cview-edit-or-delete-clients-and-scopes
upvoted 1 times

AsakuraYoh 1 year, 9 months ago
Selected Answer: B
Anyone do you think base on the question the answer is Letter B?
upvoted 1 times

jitu028 1 year, 9 months ago
Selected Answer: C
Correct answer - C
https://support.google.com/a/answer/162106?hl=en#zippy=%2Cview-edit-or-delete-clients-and-scopes:~:text=View%2C%20edit%2C%20or,immediately%20stop%20working.
upvoted 2 times

Question #35 *Topic 1*

Your organization has just completed migrating users to Workspace. Many employees are concerned about their legacy Microsoft Office documents, including issues of access, editing, and viewing. Which two practices should you use to alleviate user concerns without limiting Workspace collaboration features? (Choose two.)

A. Configure Context-Aware Access policies to block access to Microsoft Office applications.

B. Demonstrate the ability to convert Office documents to native Google file format from Drive.

C. Demonstrate and train users to use the Workspace Migrate tool.

D. Deliver training sessions that show the methods to access and edit native Office files in Drive, the Workspace file editors, and Drive for Desktop.

E. Continue to use installed Office applications along with Google Drive for Desktop.

Suggested Answer: *AD*

Community vote distribution

BD (100%)

jitu028 Highly Voted 1 year, 9 months ago

Selected Answer: BD

Correct answer - BD

upvoted 9 times

impearl Highly Voted 1 year, 9 months ago

Answer is B,D

upvoted 5 times

05fe736 Most Recent 2 months, 2 weeks ago

Selected Answer: BD

B & D would alleviate user concerns without limiting Workspace collaboration features.

upvoted 1 times

virat_kohli 10 months, 1 week ago

Selected Answer: BD

B. Demonstrate the ability to convert Office documents to native Google file format from Drive.

D. Deliver training sessions that show the methods to access and edit native Office files in Drive, the Workspace file editors, and Drive for Desktop.

upvoted 1 times

Gomesallef 11 months, 2 weeks ago

Selected Answer: BD

B. Demonstrate the ability to convert Office documents to native Google file format from Drive.

D. Deliver training sessions that show the methods to access and edit native Office files in Drive, the Workspace file editors, and Drive for Desktop.

upvoted 1 times

amministrazione 11 months, 3 weeks ago

B. Demonstrate the ability to convert Office documents to native Google file format from Drive.

D. Deliver training sessions that show the methods to access and edit native Office files in Drive, the Workspace file editors, and Drive for Desktop.

upvoted 1 times

Prosecute 1 year, 1 month ago

Selected Answer: BD

BD is obvious

upvoted 1 times

[Removed] 1 year, 2 months ago

Selected Answer: BD

BD is correct for me

upvoted 1 times

jdosh 1 year, 3 months ago

Selected Answer: BD

B&D are correct but D&E is also okay because drive for desktop has "Real-time presence in Microsoft Office"

upvoted 1 times

jaxclain 1 year, 9 months ago

Selected Answer: BD

B and D are correct.

upvoted 3 times

Question #36 *Topic 1*

Your IT team is being asked to fulfill a query by your organization's legal department that requires an MBOX file that will be shared to a third-party partner for eDiscovery. The query must be run on multiple users. Legal has no admin rights to Google Vault. What should you do to fulfil the request?

A. Create a Google Vault matter for each user account, and share the matters to the legal admin.

B. Create a Google Vault matter, search for data, and run an export for the legal department.

C. Use the Investigation Too! to search for the data requested, and export for the legal department.

D. Search for the data in Gmail, and export for the legal department.

Suggested Answer: *B*

Community vote distribution

B (100%)

virat_kohli 10 months, 1 week ago

Selected Answer: B

B. Create a Google Vault matter, search for data, and run an export for the legal department.

upvoted 1 times

Gomesallef 11 months, 2 weeks ago

Selected Answer: B

B. Create a Google Vault matter, search for data, and run an export for the legal department.

upvoted 1 times

amministrazione 11 months, 3 weeks ago

B. Create a Google Vault matter, search for data, and run an export for the legal department.

upvoted 1 times

Steventjie 1 year ago

Did you guys spot the "Investigation Too!"?

upvoted 1 times

karl19 1 year, 3 months ago

Selected Answer: B

To fulfill the request from the legal department for an MBOX file that will be shared with a third-party partner for eDiscovery, and considering that the legal department has no admin rights to Google Vault, the recommended approach is:

B. Create a Google Vault matter, search for data, and run an export for the legal department.

Explanation:

Creating a Google Vault matter (option B) allows you to specify the scope of the search and export for multiple user accounts. You can define the search criteria based on the query from the legal department and run the export to generate an MBOX file containing the relevant data.
Google Vault provides advanced search capabilities and ensures the preservation and integrity of the data during the eDiscovery process. It is designed specifically for legal and compliance needs, making it the appropriate tool for this scenario.

upvoted 3 times

jaxclain 1 year, 9 months ago

Selected Answer: B

B is correct, the question specify you need an MBOX file so you have to export the results to an MBOX file and send it to the legal department.

upvoted 2 times

RJRF503 1 year, 9 months ago

Selected Answer: B

B

As it's asking you to share an MBOX file.

https://support.google.com/vault/answer/2473458?hl=en

upvoted 2 times

jitu028 1 year, 9 months ago

Selected Answer: B

correct answer - B

https://www.youtube.com/watch?v=D5qKC90sLu8

upvoted 1 times

Question #37 *Topic 1*

Your organization is using Password Sync to sync passwords from Active Directory to Google Workspace. A user changed their network password and cannot log in to Google Workspace with the new password. What steps should you take to troubleshoot this issue?

A. Reinstall Password Sync on all domain controllers.

B. Reauthorize the Password Sync tool in the Google Workspace Admin Console.

C. Confirm that the Password Sync service is running on all domain controllers.

D. Reset the user's password in Active Directory.

Suggested Answer: *B*

Community vote distribution

C (79%) D (17%)

jitu028 Highly Voted 1 year, 9 months ago

Selected Answer: C

Correct answer - C

https://www.youtube.com/watch?v=P-r8bvivZuM

upvoted 8 times

virat_kohli Most Recent 10 months, 1 week ago

Selected Answer: C

C. Confirm that the Password Sync service is running on all domain controllers.

upvoted 1 times

Gomesallef 11 months, 1 week ago

Selected Answer: C

Correct answer - C

upvoted 1 times

amministrazione 11 months, 3 weeks ago

C. Confirm that the Password Sync service is running on all domain controllers.

upvoted 1 times

Jane1234YIP 1 year, 1 month ago

Selected Answer: C

Password Sync is a service used to synchronize passwords from Active Directory to Google Workspace (formerly known as G Suite) accounts. If a user changes their network password, and it doesn't sync to Google Workspace, there might be an issue with the Password Sync service.

upvoted 1 times

[Removed] 1 year, 2 months ago

Selected Answer: B

B active directory is working thats why the user was able to change their password... it needs to be reathorised

upvoted 1 times

NoName2546 1 year, 2 months ago

Selected Answer: C

You need to install password sync on all domain controllers, if an User changes it's password and it doesn't change on Workspace, the problem might be that the Domain Controller that handled the password change didn't have Password Sync installed.

https://support.google.com/a/answer/2611859?hl=en&ref_topic=4498019&fl=1&sjid=15192495995062168443-NA

upvoted 1 times

jdosh 1 year, 3 months ago

Selected Answer: C

C, thanks to jitu028 video

upvoted 1 times

karl19 1 year, 3 months ago

Selected Answer: D

D. Reset the user's password in Active Directory.

When a user changes their network password, the change needs to be synchronized with Google Workspace through Password Sync.
Resetting the user's password in Active Directory (option D) ensures that the updated password is synced to Google Workspace. This step allows the user to log in to Google Workspace using their new password.

upvoted 1 times

Willem_M 1 year, 9 months ago

Selected Answer: C

Changing your network password should in turn change your AD password on the DC you are connected to, it can take some time for it to transfer to other DC's too. I think that you should install the sync tool on all DC's to mitigate this issue.

upvoted 2 times

jaxclain 1 year, 9 months ago

Selected Answer: D

"Network Password" lol I believe is not the same as the Active Directory password so I would go for option D

upvoted 1 times

RAZKZ 1 year, 9 months ago

Oh no... now we have to wonder if they just suck at writing the question and they meant AD password or not.

Yeah... if it was AD password it would have been C for sure, but not network password.

upvoted 1 times

Exam__ 1 year, 9 months ago

Selected Answer: C

Correct is option C

upvoted 1 times

certificationDJJ 1 year, 9 months ago

Selected Answer: C

Reason: The network password is determined to be with AD. In this case, you must verify that password sync is installed on all domain controllers. This is the initial troubleshooting. After this troubleshooting, the logs of these connectors are taken

upvoted 3 times

RJRF503 1 year, 9 months ago

Selected Answer: D

D
The user changed their network password which is not the same as the Active Directory password.
For Password Sync to synchronize a Microsoft Active Directory (AD) password with a user's Google Workspace or Cloud Identity account, your users must change their Active Directory password.
https://support.google.com/a/answer/11237847?hl=en&ref_topic=4498019

upvoted 2 times

certificationDJJ 1 year, 9 months ago

Correct is option C

Reason: The network password is determined to be with AD. In this case, you must verify that password sync is installed on all domain controllers. This is the initial troubleshooting. After this troubleshooting, the logs of these connectors are taken

upvoted 1 times

Question #38 *Topic 1*

Your sales team, which is organized as its own organizational unit, is prone to receiving malicious attachments. What action should you take, as an administrator, to apply an additional layer of protection in the admin console for your sales team without disrupting business operation?

A. Configure an attachment compliance rule to send any emails with attachments received by users within the sales team organizational unit to an administrator quarantine.

B. Configure an attachment compliance rule to strip any attachments received by users within the sales team organizational unit.

C. Configure the security sandbox feature on the sales team organizational unit.

D. Update the Email Allowlist in the admin console to only include IP addresses of known senders.

Suggested Answer: *B*

Community vote distribution

C (94%) 6%

virat_kohli 10 months, 1 week ago

Selected Answer: C

C. Configure the security sandbox feature on the sales team organizational unit.

upvoted 1 times

Gomesallef 11 months, 1 week ago

Selected Answer: C

correct letter C. Configure the security sandbox feature on the sales team organizational unit.

upvoted 1 times

amministrazione 11 months, 3 weeks ago

C. Configure the security sandbox feature on the sales team organizational unit.

upvoted 1 times

Steventjie 1 year ago

Selected Answer: A

So it's fine for the sales team to never ever receive any attachments via email? I'm certain there would be plenty valid circumstances where they would need to receive attachments via email, A makes the most sense to me tbh.

upvoted 1 times

danaracena 1 year, 1 month ago

Selected Answer: C

Says they are PRONE to receive malicious attachments, so we are not looking to block all of them. Says also that is required an ADITIONAL layer of security, and also NOT DISRUPT THE BUSINESS OPERATION ... Option B doesnt furfill any of the requirements. Is a drastic solution, doesnt discriminate and impacts
the business.

upvoted 3 times

Bardapapa 1 year, 2 months ago

the security sandbox feature doesn't work for all licences types. So C is not the correct answer.

upvoted 1 times

karl19 1 year, 3 months ago

Selected Answer: C

By enabling the security sandbox feature, attachments that are flagged as potentially harmful can be opened and examined within a controlled environment. This helps to mitigate the risk of malware or other malicious content affecting the user's system.

upvoted 1 times

pid 1 year, 6 months ago

Selected Answer: C

I don't know how Sales will be able to get non- threatening attachments if they are stripped and sent to quarantine. Admin will have to forward one by one. Security sandbox makes more sense

upvoted 2 times

jaxclain 1 year, 9 months ago

Selected Answer: C

I agree, answer should be Security Sandbox (C) but there is already another question with Security Sandbox so this is confusing lol but for sure it has to be Security Sandbox, makes no sense to send the email to a quarantine so the admin can open it? the security sandbox will scan the file in a secure zone so it is way better.

upvoted 3 times

jitu028 1 year, 9 months ago

Selected Answer: C

correct answer - C

https://support.google.com/a/answer/7676854?hl=en#:~:text=As%20an%20administrator,malicious%20attachments.

upvoted 4 times

Question #39 *Topic 1*

Your organization does not allow users to share externally. The security team has recently approved an exemption for specific members of the marketing team and sales to share documents with external customers, prospects, and partners. How best would you achieve this?

A. Create a configuration group with the approved users as members, and use it to create a target audience.

B. Enable external sharing for the marketing and sales organizational units.

C. Enable external sharing only to allowlisted domains provided by marketing and sales teams.

D. Create a configuration group with the approved users as members, and enable external sharing for this group.

Suggested Answer: *D*

Community vote distribution

D (85%) C (15%)

jitu028 Highly Voted 1 year, 9 months ago

Selected Answer: D

Correct answer - D

https://support.google.com/a/answer/9224126?hl=en#zippy=%2Coptions-for-configurations-groups:~:text=Using%20configurations%20groups,of%20your%20organization.

upvoted 7 times

virat_kohli Most Recent 10 months, 1 week ago

Selected Answer: D

D. Create a configuration group with the approved users as members, and enable external sharing for this group.

upvoted 1 times

Gomesallef 11 months ago

Selected Answer: C

rectifying please!!!

Correct answer - D

Letter B would also be correct.

upvoted 1 times

Gomesallef 11 months, 1 week ago

Selected Answer: C

Correct answer - D

upvoted 1 times

amministrazione 11 months, 3 weeks ago

D. Create a configuration group with the approved users as members, and enable external sharing for this group.

upvoted 1 times

BearPop 1 year, 1 month ago

Selected Answer: D

D seems correct

upvoted 1 times

karl19 1 year, 3 months ago

D: Create a configuration group with the approved users as members and enable external sharing for this group.

By creating a configuration group and adding the approved users as members, you can apply specific settings and permissions to that group. In this case, you would enable external sharing specifically for this group, allowing the members of the marketing and sales teams to share documents with external customers, prospects, and partners.

This approach ensures that only the approved users have the ability to share externally, while the rest of the organization remains

restricted from external sharing. It provides a granular level of control and allows you to manage external sharing permissions for specific groups or individuals.

upvoted 1 times

jaxclain 1 year, 9 months ago

Selected Answer: D

D seems correct

upvoted 2 times

Question #40 *Topic 1*

As a Workspace Administrator, you want to keep an inventory of the computers and mobile devices your company owns in order to track details such as device type and who the device is assigned to. How should you add the devices to the company-owned inventory?

A. Download the company owned inventory template CSV file from the admin panel, enter the serial number of the devices, and upload it back to the company owned inventory in the admin panel.

B. Download the company owned inventory template CSV file from the admin panel, enter the Device OS, serial number and upload it back to the company owned inventory in the admin panel.

C. Download the company owned inventory template CSV file from the admin panel, enter the asset tag of the devices, and upload it back to the company owned inventory in the admin panel.

D. Download the company owned inventory template CSV file from the admin panel, enter the Device OS, asset tag and upload it back to the company owned inventory in the admin panel.

Suggested Answer: *A*

Community vote distribution

A (100%)

jaxclain Highly Voted 1 year, 9 months ago

Selected Answer: A

Agreed, A is correct, is not mandatory to include anything else, just need the Serial Number of the device and if you want to include the Asset Tag is optional, here is the documentation: https://support.google.com/a/answer/7129612?hl=en&fl=1

upvoted 8 times

jitu028 Highly Voted 1 year, 9 months ago

Selected Answer: A

Correct answer - A

https://support.google.com/a/answer/7129612?hl=en#zippy=%2Cassigning-devices%2Cadd-android-devices-for-the-most-management-features:~:text=Add%20devices%20to,and%20upload%20status.

upvoted 5 times

virat_kohli Most Recent 10 months, 1 week ago

Selected Answer: A

A. Download the company owned inventory template CSV file from the admin panel, enter the serial number of the devices, and upload it back to the company owned inventory in the admin panel.

upvoted 1 times

Gomesallef 11 months, 1 week ago

Selected Answer: A

Correct answer - A

https://support.google.com/a/answer/7129612?hl=en#zippy=%2Cassigning-devices%2Cadd-android-devices-for-the-most-management-features:~:text=Add%20devices%20to,and%20upload%20status.

upvoted 1 times

amministrazione 11 months, 3 weeks ago

A. Download the company owned inventory template CSV file from the admin panel, enter the serial number of the devices, and upload it back to the company owned inventory in the admin panel.

upvoted 1 times

BearPop 1 year, 1 month ago

Selected Answer: A

I would go with A

upvoted 1 times

karl19 1 year, 3 months ago

Selected Answer: A

A. Download the company owned inventory template CSV file from the admin panel, enter the serial numbers of the devices, and upload it back to the company owned inventory in the admin panel.

This option aligns with the provided steps for adding devices to the inventory in the Google Admin console. It emphasizes the requirement to enter the serial numbers of the devices, which is the key piece of information needed for tracking the devices in the inventory.

upvoted 3 times

Question #41 *Topic 1*

When reloading Gmail in Chrome, the web browser returns a 500 Error. As part of the troubleshooting process, Google support asks you to gather logs. How can this be accomplished?

A. Chrome > Window Context Menu > More Tools > Developer Tools > Network Tab > Reload the page to replicate the error > “Export HAR”

B. Admin.google.com > Reporting > Reports > Apps Reports > Gmail

C. chrome://net-export > Start Logging to Disk > Confirm validity with https://netlog-viewer.appspot.com

D. Chrome > Window Context Menu > More Tools > Task Manager > Screen Capture List of Running Processes

Suggested Answer: *A*

Community vote distribution

A (100%)

virat_kohli 10 months, 1 week ago

Selected Answer: A

A. Chrome > Window Context Menu > More Tools > Developer Tools > Network Tab > Reload the page to replicate the error > “Export HAR”

upvoted 1 times

karl19 1 year, 3 months ago

Selected Answer: A

A. Chrome > Window Context Menu > More Tools > Developer Tools > Network Tab > Reload the page to replicate the error > “Export HAR”

This option allows you to access the Developer Tools in Chrome and gather network logs using the "Export HAR" feature. HAR (HTTP Archive) is a file format that contains information about the interactions between a web browser and a website. By exporting the HAR file, you can provide Google support with detailed logs that can help in troubleshooting the 500 Error in Gmail.

upvoted 1 times

jaxclain 1 year, 9 months ago

Selected Answer: A

Easy, answer is A, you can even Google it and you will find the same steps.

upvoted 1 times

jitu028 1 year, 9 months ago

Selected Answer: A

correct answer - A

chrome://settings/syncSetup

upvoted 3 times

Question #42 *Topic 1*

Your company is using Google Workspace Business Standard. The company has five meeting rooms that are all registered as resources in Google Workspace and used on a daily basis by the employees when organizing meetings. The office layout was changed last weekend, and one of the meeting rooms is now a dedicated room for management. The CEO is complaining that anyone can book the room and requested this room to be used only by the management team and their executive assistants (EAs). No one else must be allowed to book it via Google Calendar. What should you do?

A. As a super administrator, modify the room calendar sharing settings, and limit it to the management and EAs group.

B. Delete the room from Google Workspace resources, and suggest using a spreadsheet shared with the management and EAs only for the room schedule.

C. As a super administrator, create a group calendar named “Management Room,” and share it only with the management and the EAs.

D. Move the room resource to the management and EAs group so that only they can use it.

Suggested Answer: *C*

Community vote distribution

A (90%) 10%

jaxclain Highly Voted 1 year, 9 months ago

Selected Answer: A

Option A is correct, I also had a similar question on my Deployment Specialist test and I was able to see if the answer was right, you need an Administrator account with Calendar management privileges to do this, here is the documentation: https://support.google.com/a/answer/1034381?hl=en

upvoted 5 times

virat_kohli Most Recent 10 months, 1 week ago

Selected Answer: A

A. As a super administrator, modify the room calendar sharing settings, and limit it to the management and EAs group.

upvoted 1 times

[Removed] 1 year, 2 months ago

there is no need to create or modify..you simply have to move it to the OU of manaement and EAs. a user from a different ou wont be able to see it so they can book

upvoted 1 times

karl19 1 year, 3 months ago

Selected Answer: A

A. As a super administrator, modify the room calendar sharing settings and limit it to the management and EAs group.

To restrict the booking of the meeting room to only the management team and their executive assistants (EAs), you can modify the room calendar's sharing settings. As a super administrator, you can specify that only the management and EAs group has permission to book the room via Google Calendar. By limiting the sharing settings in this way, only members of the designated group will be able to schedule the management room for meetings.

upvoted 1 times

Exam__ 1 year, 9 months ago

Selected Answer: A

correct answer - A

upvoted 1 times

RAZKZ 1 year, 9 months ago

Wouldn't that change the settings for the entire calendar rooms? they want to limit one room right?

upvoted 1 times

RAZKZ 1 year, 9 months ago

Is the "room calendar" a name for "calendar resource"? that's so not obvious, the docs mention them as resources.

upvoted 1 times

certificationDJJ 1 year, 9 months ago

Selected Answer: A

Since he is sitting in the room, this case fits best for the organization.

upvoted 1 times

jitu028 1 year, 9 months ago

changing answer to - A

need change to room sharing setting instead

upvoted 1 times

jitu028 1 year, 9 months ago

Selected Answer: C

correct answer - C

upvoted 1 times

Question #43 *Topic 1*

You act as the Google Workspace Administrator for a company that has just acquired another organization. The acquired company will be migrated into your Workspace environment in 6 months. Management has asked you to ensure that the Google Workspace users you currently manage can efficiently access rich contact information in Workspace for all users. This needs to occur before the migration, and optimally without additional expenditure. What step do you take to populate contact information for all users?

A. Bulk-upload the contact information for these users via CSV into the Google Directory.

B. Use the Domain Shared Contacts API to upload contact information for the acquired company's users.

C. Provision and license Google Workspace accounts for the acquired company's users because they will need accounts in the future.

D. Prepare an uploadable file to be distributed to your end users that allows them to add the acquired company's user contact information to their personal contacts.

Suggested Answer: *D*

Community vote distribution

B (93%) 7%

csavar 2 weeks, 2 days ago

still thinks that A can be a good choice...

upvoted 1 times

md111111 5 months ago

Hello, why not option A? Is it because it requires paying licenses before the actual migration?

upvoted 1 times

virat_kohli 10 months, 1 week ago

Selected Answer: B

B. Use the Domain Shared Contacts API to upload contact information for the acquired company's users.

upvoted 1 times

karl19 1 year, 3 months ago

Selected Answer: B

B: Use the Domain Shared Contacts API to upload contact information for the acquired company's users. This option allows you to programmatically import the contact information into shared contacts that can be accessed by all users in your Google Workspace environment.

By utilizing the Domain Shared Contacts API, you can automate the process of importing contact information, ensuring consistency and reducing the risk of data leaks. This method also provides a centralized and easily accessible source of contact information for all users.

upvoted 3 times

gastonMM 1 year, 5 months ago

Selected Answer: B

Correct answer - B

upvoted 1 times

jaxclain 1 year, 9 months ago

Selected Answer: B

100% sure is option B, here is the documentation: https://support.google.com/a/answer/9281635?hl=en

upvoted 4 times

Exam__ 1 year, 9 months ago

Selected Answer: B

Correct answer - B

upvoted 1 times

HM2H 1 year, 9 months ago

Answer - B

The Domain Shared Contacts API lets your applications get and update external contacts that are shared with all users in a Google Workspace domain. Shared contacts are visible to all users of a Google Workspace domain and all Google services have access to the contact list

https://developers.google.com/admin-sdk/domain-shared-contacts/overview

upvoted 2 times

certificationDJJ 1 year, 9 months ago

Selected Answer: B

cannot have costs. The best choice would be:

https://developers.google.com/admin-sdk/domain-shared-contacts

upvoted 3 times

jitu028 1 year, 9 months ago

Selected Answer: A

Correct answer - A

https://support.google.com/a/answer/6191788?hl=en#:~:text=Update%20many%20profiles%20from,users%20at%20once.

upvoted 1 times

Question #44 *Topic 1*

Your organization is about to expand by acquiring two companies, both of which are using Google Workspace. The CISO has mandated that strict 'No external content sharing' policies must be in place and followed. How should you securely configure sharing policies to satisfy both the CISO's mandate while allowing external sharing with the newly acquired companies?

A. Allow external sharing of Drive content for the IT group only.

B. Create a Drive DLP policy that will allow sharing to only domains on an allowlist.

C. Use shared drives to store the content, and share only individual files externally.

D. Let users share files between the two companies by using the 'Trusted Domains' feature. Create an allowlist of the trusted domains, and choose sharing settings for the users.

Suggested Answer: *D*

Community vote distribution

D (90%) 10%

virat_kohli 10 months, 1 week ago

Selected Answer: D

D. Let users share files between the two companies by using the 'Trusted Domains' feature. Create an allowlist of the trusted domains, and choose sharing settings for the users.

upvoted 1 times

[Removed] 1 year, 2 months ago

Selected Answer: B

Create a Drive Data Loss Prevention policy that will allow sharing to only domains on an allowlist.

upvoted 1 times

karl19 1 year, 3 months ago

Selected Answer: D

Option D: Let users share files between the two companies using the 'Trusted Domains' feature. Create an allowlist of the trusted domains and choose sharing settings for the users.

By using the 'Trusted Domains' feature, you can specify the domains that are allowed for external sharing while restricting sharing with other domains. This allows users from the newly acquired companies to share files and collaborate with your organization, while still maintaining strict restrictions on general external content sharing.

This approach provides a controlled and secure environment for sharing files between the two organizations, as the sharing is limited to the trusted domains specified in the allowlist.

upvoted 3 times

jaxclain 1 year, 9 months ago

Selected Answer: D

D for sure

upvoted 3 times

jitu028 1 year, 9 months ago

Selected Answer: D

Correct answer - D

https://support.google.com/a/answer/6160020?hl=en#zippy=%2Cgive-sharing-access-to-trusted-domains:~:text=only%20trusted%20domains-,Allow%20external%20sharing%20with%20only%20trusted%20domains,-Help%20and%20tips

upvoted 2 times

Question #45 *Topic 1*

Your company is using Google Workspace Enterprise Plus, and the Human Resources (HR) department is asking for access to Work Insights to analyze adoption of Google Workspace for all company employees. You assigned a custom role with the work Insights permission set as “view data for all teams” to the HR group, but it is reporting an error when accessing the application. What should you do?

A. Allocate the “view data for all teams” permission to all employees of the company.

B. Confirm that the Work Insights app is turned ON for all employees.

C. Confirm in Security > API controls > App Access Controls that Work Insights API is set to “unrestricted.”

D. Confirm in Reports > BigQuery Export that the job is enabled.

Suggested Answer: *C*

Community vote distribution

B (74%) C (26%)

jaxclain Highly Voted 1 year, 8 months ago

Selected Answer: B

Correcting myself here, after reviewing the question a second time.. i go for option B.. first here is the documentation of the View data for all teams priviledge: https://support.google.com/a/answer/9135419?fl=1#zippy=%2Cstep-understand-work-insights-privileges

Then here is the documentation about turning the service On and it mentions, it will not have access unless the appropiate privilege is granted, so it already has the correct privilege, just need to confirm that the app is on: https://support.google.com/a/answer/9135183?fl=1#zippy=%2Cstep-turn-work-insights-on-or-off-for-organizational-units

I was able to test on an Enterprise edition and this is the correct answer because I did not find it under API controls > apps.. or not sure if I did it incorrectly but indeed B seems correct here.

upvoted 5 times

virat_kohli Most Recent 10 months, 1 week ago

Selected Answer: B

B. Confirm that the Work Insights app is turned ON for all employees.

upvoted 1 times

[Removed] 1 year, 1 month ago

Selected Answer: C

the error being highlighted suggests a restriction issue

upvoted 1 times

jdosh 1 year, 3 months ago

Selected Answer: B

B is correct, work insight is not in the app access control so you cannot set it to restricted or unrestricted.

upvoted 3 times

karl19 1 year, 3 months ago

Selected Answer: B

Option B, "Confirm that the Work Insights app is turned ON for all employees," would indeed be the appropriate step to take in this scenario. By ensuring that the Work Insights app is enabled for all employees, you are allowing them to access and use the app to analyze adoption data for Google Workspace. Enabling the app ensures that all necessary permissions and access are granted for Work Insights functionality.

upvoted 1 times

Moss2011 1 year, 8 months ago

Selected Answer: B

The answer is B because there is no Work Insights (only available in the Enterprise Plus Edition) API inside the given path

upvoted 4 times

hehe_24 1 year, 8 months ago

Security > access and data control > api control > app access control > work insights api not found under manage google services. So I will go with option B.

upvoted 3 times

hehe_24 1 year, 8 months ago

Note that I have enterprise plus license in test env

upvoted 1 times

jaxclain 1 year, 9 months ago

Selected Answer: C

C is correct, the options A and D makes no sense, with option B we have to assume that Work Insights is already on and this is why they get the error so just make sure from the API is set to unrestricted.

https://support.google.com/a/answer/9135419?hl=en

upvoted 2 times

jitu028 1 year, 9 months ago

Selected Answer: C

Correct answer - C

upvoted 2 times

RAZKZ 1 year, 9 months ago

I can't even find work insights under App access control in security under managed services.

upvoted 1 times

jaxclain 1 year, 9 months ago

Maybe you don't have the correct License but C is correct.

upvoted 2 times

jdosh 1 year, 3 months ago

Nope, work insight is not in the app access control we are on Enterprise Plus buddy.

upvoted 1 times

Question #46 *Topic 1*

You received this email from the head of marketing:
Hello Workspace Admin:
Next week, a new consultant will be starting on the “massive marketing mailing” project. We want to ensure that they can view contact details of the rest of the marketing team, but they should not have access to view contact details of anyone else here at our company. Is this something that you can help with?
What are two of the steps you need to perform to fulfill this request? (Choose two.)

A. Create an isolated OU for the consultants who need the restricted contacts access.

B. Create a group that includes the contacts that the consultant is allowed to view.

C. Apply the role of owner to the consultant in the group settings.

D. Create the consultant inside under the marketing OU.

E. Ensure that you have the Administrator Privilege of Services > Services settings and that Services > Contacts > Contacts Settings Message is set.

Suggested Answer: *B,E*

Community vote distribution

AB (100%)

virat_kohli 10 months, 1 week ago

Selected Answer: AB

A. Create an isolated OU for the consultants who need the restricted contacts access.
B. Create a group that includes the contacts that the consultant is allowed to view.
upvoted 1 times

jdosh 1 year, 2 months ago

Selected Answer: AB

A and B are the only things that make sense.
upvoted 1 times

karl19 1 year, 3 months ago

Selected Answer: AB

Option A: Create an isolated OU for the consultants who need restricted contacts access: By creating a separate organizational unit (OU) specifically for the consultants, you can apply different access policies and permissions to that OU. This allows you to control the visibility of contact details for the marketing team while restricting access to other company contacts.

Option B: Create a group that includes the contacts the consultant is allowed to view: Create a group specifically for the marketing team contacts that the consultant should be able to access. Add the relevant marketing team members to this group. By granting access to this group, the consultant will be able to view the contact details of the marketing team members.

Please note that options C, D, and E are not directly related to fulfilling the request mentioned in the email and are not necessary for achieving the desired outcome.
upvoted 4 times

jcloud965 10 months, 3 weeks ago

Best explanation
upvoted 1 times

stickline 1 year, 3 months ago

Selected Answer: AB

looks like AB is right
upvoted 1 times

Exam__ 1 year, 9 months ago

should be AB
upvoted 1 times

impearl 1 year, 9 months ago

Selected Answer: AB

https://support.google.com/a/answer/7566446?hl=en&fl=1

upvoted 1 times

RAZKZ 1 year, 9 months ago

You mentioned A/B, but also B/D.

I'm also quite confused on this question, you need the permissions but you also need to create OU & Group, which one is it?

upvoted 1 times

impearl 1 year, 9 months ago

B, D

https://support.google.com/a/answer/7566446?hl=en&fl=1

upvoted 4 times

jdosh 1 year, 2 months ago

D is wrong, you will restrict all the marketing OU users from seeing the other users in the domain if you do that.

upvoted 2 times

Question #47 *Topic 1*

A disgruntled employee has left your company and deleted all their email messages and files in Google Drive. The security team is aware that some intellectual property may have surfaced on a public social media site. What is the first step to start an investigation into this leak?

A. Delete the user's account in the Admin Console.

B. Transfer data between end user Workspace accounts.

C. Instruct a Google Vault admin to create a matter, and place all the user data on 'hold.'

D. Use Google Vault to export all the user data and share among the security team.

Suggested Answer: *D*

Community vote distribution

C (100%)

jaxclain Highly Voted 1 year, 9 months ago

Selected Answer: C

If it was me, I would just search for the users data then share it with the security team.
If there is not any retention policy applied then yes a Hold but most companies have Vault retention to indefinite so there is no need to use a Hold but for this question (bad elaborated) then yes, the correct answer is C, because there is no mention of what retention policies they are using.

https://support.google.com/vault/answer/7664657?hl=en#zippy=%2Cwhats-the-difference-between-a-hold-and-a-retention-rule

upvoted 5 times

05fe736 Most Recent 2 months, 2 weeks ago

Selected Answer: C

As a "first step to start an investigation into this leak" it sounds like creating a matter and placing ALL the user data on hold would be correct.

upvoted 1 times

virat_kohli 10 months, 1 week ago

Selected Answer: C

C. Instruct a Google Vault admin to create a matter, and place all the user data on 'hold.'

upvoted 1 times

danaracena 1 year, 1 month ago

Selected Answer: C

First proper step is to create the investigation. If the question was "There's an emergency and need to check information right away" could be D. But as a first adecuate, secure, and auditable step. Must create the hold first.

upvoted 1 times

karl19 1 year, 3 months ago

Selected Answer: C

The first step to start an investigation into the potential intellectual property leak is:

C. Instruct a Google Vault admin to create a matter and place all the user data on 'hold.'

By creating a matter in Google Vault and placing the user's data on hold, you ensure that any relevant information related to the disgruntled employee's actions is preserved and cannot be modified or deleted. This allows the security team to analyze the data and investigate the potential leak.

upvoted 2 times

stickline 1 year, 3 months ago

Selected Answer: C

Agree with C

upvoted 1 times

jitu028 1 year, 9 months ago

Selected Answer: C

correct answer - C

upvoted 2 times

Question #48 *Topic 1*

Users in your organization are routinely complaining that they receive messages containing words of profanity they find inappropriate in a professional setting. As the administrator, what steps should you take to prevent the messages from being delivered to users' mailboxes?

A. Configure an objectionable content rule.

B. Configure an attachment compliance rule.

C. Enable optical character recognition (OCR).

D. Set up a Gmail DLP policy.

Suggested Answer: *A*

Community vote distribution

A (100%)

Mauricio1993 Highly Voted 1 year, 1 month ago

Selected Answer: A

A is correct

https://support.google.com/a/answer/1346936?hl=en

upvoted 5 times

virat_kohli Most Recent 10 months, 1 week ago

Selected Answer: A

A. Configure an objectionable content rule.

upvoted 1 times

Question #49 *Topic 1*

A user joined your organization and is reporting that every time they start their computer they are asked to sign in. This behavior differs from what other users within the organization experience. Others are prompted to sign in biweekly. What is the first step you should take to troubleshoot this issue for the individual user?

A. Reset the user's sign-in cookies.

B. Confirm that this user has their employee ID populated as a sign-in challenge.

C. Check the session length duration for the organizational unit the user is provisioned in.

D. Verify that 2-Step Verification is enforced for this user.

Suggested Answer: *D*

Community vote distribution

C (50%) B (40%) 10%

professionalCrammer23 5 months, 3 weeks ago

Selected Answer: C

Answer is C. Check that the session length is configured correctly first.

upvoted 1 times

virat_kohli 10 months, 1 week ago

Selected Answer: C

C. Check the session length duration for the organizational unit the user is provisioned in.

upvoted 1 times

jcloud965 10 months, 3 weeks ago

Selected Answer: C

Session length can be as short as 1 hour and explain the behavior.

It can be a cookies issue but clearing them will have an impact on the user experience.

upvoted 1 times

ChizTheWhiz 11 months ago

Correction, A will logout the user. B is for login challenge and this is disabled by default so C is the most feasible answer.

upvoted 1 times

ChizTheWhiz 11 months ago

C is correct. as B will just logout the user on devices as per this article - https://apps.google.com/supportwidget/articlehome?hl=en&article_url=https%3A%2F%2Fsupport.google.com%2Fa%2Fanswer%2F2537800%3Fhl%3Den&assistant_id=generic-unu&product_context=2537800&product_name=UnuFlow&trigger_context=a

upvoted 2 times

Richard_Bagson 11 months, 2 weeks ago

The FIRST STEP should absolutely be to clear the user's cookies. Especially seeing as the issue is affecting just one user, it is most likely to be an issue specific to the browser session on that user's machine. I would try the other steps after first clearing cookies. I think the correct answer is A.

upvoted 1 times

jcloud965 10 months, 3 weeks ago

The first step should be to check if this is intended behavior = C

Clearing cookies will have an impact on the user experience.

upvoted 1 times

cloudguy2 11 months, 3 weeks ago

Correct answer is C - checking the session length. User may be in an OU w/more rigid (less than 24 hours) while other in the org session length is 14 days https://support.google.com/a/answer/7576830?hl=en&fl=1&sjid=18033713616032115750-NA

upvoted 3 times

ryuhei 1 year, 1 month ago

Selected Answer: B

Answer is B !?

upvoted 1 times

cloudguy2 11 months, 3 weeks ago

B is not correct as login challenge is only used when Google detects suspicious activity. ? indicates this is normal behavior not suspicious AND login challenge can be disabled by default for the org. correct answer is C "session length".

upvoted 1 times

userX100 1 year, 1 month ago

Selected Answer: C

"Session length duration for the organizational unit the user is provisioned in" is the only policy that applies in this case.

upvoted 1 times

Jane1234YIP 1 year, 1 month ago

Selected Answer: A

If a user is experiencing an issue where they are prompted to sign in every time they start their computer, while other users are prompted biweekly, it's likely a problem with their sign-in cookies. Sign-in cookies are used to keep users signed in for a certain duration, so they don't have to enter their credentials repeatedly during that period.

Option A is the first step to troubleshoot this issue

upvoted 1 times

klu23 1 year, 1 month ago

Selected Answer: C

only C seems logical to me / first thing I would check in this case

upvoted 1 times

[Removed] 1 year, 2 months ago

Selected Answer: B

Correct answer is B. No where did the question indicate that they're using 2fa. This user is new so maybe his ID isnt on the sign-in challenge

upvoted 3 times

Question #50 *Topic 1*

Your organization has a new security requirement around data exfiltration on iOS devices. You have a requirement to prevent users from copying content from a Google app (Gmail, Drive, Docs, Sheets, and Slides) in their work account to a Google app in their personal account or a third-party app. What steps should you take from the admin panel to prevent users from copying data from work to personal apps on iOS devices? (Choose two.)

A. Clear the “allow users to copy data to personal apps” checkbox.

B. Turn on “Advanced Mobile Management.”

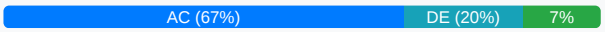
C. Navigate to Devices > Mobile and Endpoint > iOS Settings > Data Sharing > Data Protection.

D. Navigate to Devices > Mobile and Endpoint > iOS Settings > Data Sharing > Open Docs in Unmanaged Apps.

E. Clear the “allow items created with managed apps to open in unmanaged apps” checkbox.

Suggested Answer: *CE*

Community vote distribution



djdjdueufffs 4 months, 3 weeks ago

It is CE copied from Google "Allow items created with managed apps to open in unmanaged apps" Look it up yourself

upvoted 1 times

DL79 6 months, 1 week ago

Just wrote the test ...Passed. There were about 10/50 questions that were straight out of these practice questions. The other questions were a variation of these paractice questions. A+

upvoted 1 times

virat_kohli 10 months, 1 week ago

Selected Answer: AC

A. Clear the “allow users to copy data to personal apps” checkbox.

C. Navigate to Devices > Mobile and Endpoint > iOS Settings > Data Sharing > Data Protection.

upvoted 1 times

ChizTheWhiz 11 months ago

This is tricky, but based from the articles below, it could be A and E.

A - https://support.google.com/a/answer/6328700?hl=en#zippy=%2Cdata-actions

^ will prevent copying of files

E - https://support.google.com/a/answer/6328700#open_unmanaged&zippy=%2Copen-docs-in-unmanaged-apps

^ will prevent opening of files on non-work apps. If you can't open it on personal apps, then you can't copy it as A is also in place

upvoted 1 times

Richard_Bagson 11 months, 2 weeks ago

Selected Answer: BE

The correct answer is B and E. The option "Allow items created with managed apps to open in unmanaged apps" will not take effect unless mobile management is first set to Advanced. I think options C and D are there to catch you out.

upvoted 1 times

Bardapapa 1 year ago

Selected Answer: AC

B - not correct because Data protection works for basic and advanced mobile management

D- not correct - the path to E

E - not correct - they can still open docs but not copying it

upvoted 4 times

2shyshy 11 months ago

You are right, although it seems in the menu has changed to Data Actions

upvoted 2 times

joeeeee333 1 year, 1 month ago

B AND C

All these feature doesn't work unless mobile advanced management is set

upvoted 1 times

ftryn 1 year, 1 month ago

Selected Answer: AC

https://support.google.com/a/answer/6328700?hl=en#managed_apps&zippy=%2Cdata-actions

upvoted 2 times

[Removed] 1 year, 1 month ago

Selected Answer: BC

correct answer is bc...

upvoted 1 times

danaracena 1 year, 1 month ago

Selected Answer: DE

Are D,E.

Option A: exists for Android management, not IOS. B: is not because the requirement is prevent something happening, not to configure it from scratch. C: the options described doesnt even exist in console. D is the proper first step, and E the final second step.

upvoted 2 times

[Removed] 1 year, 1 month ago

do your research

upvoted 1 times

klu23 1 year, 1 month ago

Selected Answer: AC

link - https://support.google.com/a/answer/6328700?hl=en#zippy=%2Cdata-actions:~:text=Allow%20users%20to%20copy,as%20Calendar%20or%20Sites

upvoted 2 times

Prosecute 1 year, 1 month ago

Selected Answer: DE

D, E.

states from iOS devices, and exfiltration from it. You cant exfiltrate if you can't open them

upvoted 1 times

zzzzzooooo 1 year, 1 month ago

Selected Answer: AC

I guess A, C

https://support.google.com/a/answer/6328700?hl=en#data_protection

upvoted 1 times

zzzzzooooo 1 year, 1 month ago

Sorry my bad, need advanced mobile management.

Correct answers are A and B

upvoted 2 times

robbyyy 7 months, 3 weeks ago

I will vote for A C, because this docs said "advanced mobile management isn't required to use the Data actions setting."

https://support.google.com/a/answer/6328700?hl=en#management_apps&zippy=%2Capple-push-notification-service%2Capple-devic enrollment%2Cdata-actions:~:text=However%2C%20advanced%20mobile%20management%20isn%27t%20required%20to%20use%20the%20Data%20

upvoted 1 times

Question #51 *Topic 1*

You have been asked to set up a new Google Group for your Human Resources department as they onboard staff. The membership of the group will change often. The HR team and all group members need to be able to send messages to and receive messages from all members of the group. They are worried that new staff may accidentally post personal information to the group. How do you configure the Google Group to prevent onboarded staff from sharing sensitive information to all group members?

A. When provisioning the group, configure it as DLP enabled and select PII from the list of “Content Detectors”.

B. Configure the group so that members cannot view group conversations.

C. Configure the group with new member post moderation.

D. Configure the group so only Owners or Managers can post to the group.

Suggested Answer: *C*

Community vote distribution

C (100%)

virat_kohli 10 months, 2 weeks ago

Selected Answer: C

C. Configure the group with new members post moderation.

upvoted 1 times

jcloud965 10 months, 2 weeks ago

Selected Answer: C

Correct is C : Moderation. New messages must be approved by managers or owners to be sure there is no personal information posted. Member should be added using Google Groups to have the New member status instead of Google Admin.
Publication restrictions for New members should be removed by group owner or admin.

A : DLP / Content Detectors work only on outbound messages
B : "all group members need to be able to send messages to and receive messages from all members of the group". If members cannot view group conversations, they can't receive too.
D : Owners or Managers can post to the group : same as B, if members cannot post group conversations, they can't send messages.

upvoted 3 times

Mauricio1993 1 year, 1 month ago

Selected Answer: C

C -

https://support.google.com/groups/answer/2466386?hl=en&sjid=17582605696867114362-SA

upvoted 2 times

Question #52 *Topic 1*

You are the administrator for a 30,000-user organization. You have multiple Workspace licensing options available to end users in your domain, according to their work responsibilities. A user may be transitioned to a different license type multiple times in a given year. Your organization has a high turnover rate for employees. What is the most efficient way to manage your organization's licensing?

A. Use the Directory API to create a custom batch script that modifies the users license on a daily basis.

B. Create a license assignment rule in the Google Admin console to set user licensing based on directory attributes.

C. Use Google Cloud Directory Sync to modify user licensing with each sync, according to information available in the organization's LDAP.

D. Update user licensing in the user portion of the Admin console on an as-needed basis.

Suggested Answer: *C*

Community vote distribution

C (75%) B (25%)

jcloud965 Highly Voted 10 months, 2 weeks ago

Selected Answer: C

C is correct. GCDS can use different rules to assign licenses based on LDAP query. GCDS can also (un)archive users the same way.

A. The Directory API can't update license. License Manager API should be used.
B. The only assignment rule available in the Google Admin console is based on the Org Unit. There is no way to choose based on directory attributes.
D. Not efficient with 30,000 users and multiple changes in a given year

upvoted 7 times

2shyshy Highly Voted 10 months, 2 weeks ago

Why is it C if it doesn´t mention that they are using LDAP or Cloud Directory Sync. Just because of this I think it´s B.

upvoted 5 times

468fa2a Most Recent 2 weeks, 6 days ago

Selected Answer: B

I also do not think it is C because there is no reference to any LDAP solution being available, although in a 30,000 organisation is would be likely. But still....

upvoted 1 times

Nico282 8 months, 4 weeks ago

Selected Answer: C

https://support.google.com/a/answer/10148746?hl=en

You can use Google Cloud Directory Sync (GCDS) to manage and synchronize licenses for users in your Google Account.
On the Licenses page of Configuration Manager, click LDAP License Rules and then Add Rule. In the LDAP Query field, using LDAP query notation, specify the users on your LDAP directory that should be assigned the license. For details, go to Use LDAP search rules to synchronize data

upvoted 2 times

virat_kohli 10 months, 2 weeks ago

Selected Answer: C

C. Use Google Cloud Directory Sync to modify user licensing with each sync, according to information available in the organization's LDAP.

upvoted 1 times

ChizTheWhiz 11 months ago

Selected Answer: C

C is the correct answer as per this article - https://support.google.com/a/answer/10148746?hl=en

upvoted 2 times

abdulilah010 1 year ago

Selected Answer: B

I guess its B

upvoted 1 times

TQM__9MD 1 year, 1 month ago

Selected Answer: B

I think B

upvoted 2 times

joeeeee333 1 year, 1 month ago

I Guess It is B

upvoted 2 times

Question #53 *Topic 1*

Your company has numerous locations throughout the world. Each of these locations has multiple office managers that field questions from employees through an email alias. Some questions have not been answered by an office manager. How can you create a system to assign conversations to different receptionists using Workspace?

A. Create a Google Groups Collaborative Inbox.

B. Use App Script to design a ticketing system that marks conversation ownership.

C. Contract with a third-party solution, such as ServiceNow.

D. Create Google Tasks and assign them to receptionists to address unanswered questions.

Suggested Answer: *D*

Community vote distribution

A (74%) B (26%)

klu23 Highly Voted 1 year, 1 month ago

Selected Answer: A

https://support.google.com/a/users/answer/10375787?hl=en#:~:text=Sign%20in%20to%20Google%20Groups,Groups%20features%2C%20select%20Collaborative%20Inbox

upvoted 5 times

csavar Most Recent 2 weeks, 5 days ago

This definitely A

upvoted 1 times

md111111 5 months ago

Option A may work, But why not Option B?

upvoted 2 times

JessiePiper 3 months, 3 weeks ago

For testing purposes, I think it is safe to assume we should go with the native Google solution. It's also a very easy solution that doesn't require any coding knowledge or maintenance. I think this is one where, although it may not be perfect, they are looking for the "best" answer.

upvoted 1 times

virat_kohli 10 months, 2 weeks ago

Selected Answer: A

A. Create a Google Groups Collaborative Inbox.

upvoted 1 times

ChizTheWhiz 11 months ago

Selected Answer: A

Why would you do B if A (Collaborative Inbox) is existing and the features needed by the question is also there. So A.

upvoted 1 times

bobsmith69 1 year ago

Selected Answer: A

A, because B would be a custom development

upvoted 3 times

userX100 1 year, 1 month ago

Selected Answer: A

"Using Workspace" the answer should be A, because B is a custom development.

upvoted 2 times

Jane1234YIP 1 year, 1 month ago

Selected Answer: B

Option B would be the most appropriate way to create a system to assign conversations to different receptionists using Google Workspace.

upvoted 2 times

Prosecute 1 year, 1 month ago

Selected Answer: B

B, appscript is more useful for a larger set of employees

upvoted 3 times

zzzzzooooo 1 year, 1 month ago

Selected Answer: A

I guess A

upvoted 2 times

Question #54 *Topic 1*

The security team for your organization is concerned about phishing attacks against your end user base. What two actions should you take to configure the strongest possible preventative measure against phishing attacks? (Choose two.)

A. Train end users to mark messages as spam when they see something suspicious.

B. Configure spoofing and authentication controls to warn end users about messages that are perceived as threats.

C. Configure spoofing and authentication controls to quarantine messages that are perceived as threats.

D. Enforce confidential mode for all messages sent and received from your Workspace domain.

E. Force encryption on all inbound and outbound emails from your Workspace domain.

Suggested Answer: *BC*

Community vote distribution

BC (52%) CE (33%) AC (15%)

klu23 Highly Voted 1 year, 1 month ago

Selected Answer: CE

https://support.google.com/a/answer/6374496?hl=en-GB

upvoted 6 times

zanhsieh Highly Voted 11 months, 3 weeks ago

Selected Answer: BC

Vote BC.

A: No. End users won't 100% follow what Workspace admin instructions even they trained.

D: No. Confidential mode is intended for internal use. The users still need to receive emails from outside domain, such as sales shall receive customer emails.

E: No. Force encryption inbound outbound doesn't help. Phishing attacks still happen.

upvoted 6 times

dija123 Most Recent 3 months, 1 week ago

Selected Answer: BC

Agree with BC

upvoted 1 times

qtDirk 4 months ago

Selected Answer: CE

Strongest possible. SMIME Encryption and quarantining.

upvoted 1 times

djdjdueufffs 7 months, 3 weeks ago

Selected Answer: BC

Google emails are already encrypted

"Gmail messages are encrypted at rest and while in transit between data centers1.

Messages transiting to third-party providers are encrypted with Transport Layer Security when possible or required by configuration1

upvoted 1 times

virat_kohli 10 months, 2 weeks ago

Selected Answer: BC

B. Configure spoofing and authentication controls to warn end users about messages that are perceived as threats.

C. Configure spoofing and authentication controls to quarantine messages that are perceived as threats.

upvoted 1 times

jcloud965 10 months, 2 weeks ago

Selected Answer: BC

I choose B & C - even you can't do both at the same time

Others options are not accurate

upvoted 1 times

ChizTheWhiz 11 months ago

Selected Answer: BC

B, C. as even if you enforce encryption for inbound and outbound, "encrypted" phishing emails can still be sent.

upvoted 2 times

dija123 11 months ago

Selected Answer: CE

C, E make sense as strong action

upvoted 1 times

2shyshy 11 months ago

B, C are correct

upvoted 1 times

bobsmith69 1 year, 1 month ago

Selected Answer: AC

A C, Basic security question

upvoted 2 times

[Removed] 1 year, 1 month ago

Selected Answer: BC

B C for sure

upvoted 2 times

Jane1234YIP 1 year, 1 month ago

Selected Answer: BC

B. Configuring spoofing and authentication controls to warn end users about messages that are perceived as threats can help raise awareness among end users and prompt them to exercise caution when encountering suspicious emails. This warning can include banners or visual indicators that notify users about potential phishing attempts, enabling them to be more vigilant while reviewing emails.

C. Configuring spoofing and authentication controls to quarantine messages that are perceived as threats can provide an additional layer of protection. By quarantining suspicious messages, the security team can closely analyze them and determine if they are indeed phishing attempts before releasing them to end users' inboxes. This helps prevent potentially harmful messages from reaching end users until they are verified to be safe.

Options A, D, and E do not directly address phishing prevention

upvoted 3 times

danaracena 1 year, 1 month ago

Selected Answer: CE

Lets not forget that is the STRONGEST option.

upvoted 3 times

Prosecute 1 year, 1 month ago

Selected Answer: AC

A and C

upvoted 3 times

Question #55 *Topic 1*

Your organization recently bought 1,000 licenses for Cloud Identity Premium. The company's development team created an application in the enterprise service bus (ESB) that will read user data in the human resources information system (HRIS) and create accounts via the Google Directory REST API.

While doing the original test before production use, the team observes a 503 error coming from Google API response after a few users are created. The team believes the ESB is not the cause, because it can perform 100 requests per second without any problems. What advice would you give the development team in order to avoid the issue?

A. Use an exponential back-off algorithm to retry failed requests.

B. Use the domain-wide delegation API to avoid the limitation per account.

C. Use the batch request architecture, because it can pack 1,000 API calls in one HTTP request.

D. Switch from REST API to gRPC protocol for performance improvement.

Suggested Answer: *B*

Community vote distribution

A (79%) 14% 7%

virat_kohli 10 months, 2 weeks ago

Selected Answer: A

A. Use an exponential back-off algorithm to retry failed requests.

upvoted 1 times

jcloud965 10 months, 2 weeks ago

Selected Answer: A

A is the best practice

upvoted 1 times

ChizTheWhiz 11 months ago

Selected Answer: A

A is the answer

upvoted 1 times

Richard_Bagson 11 months, 2 weeks ago

Selected Answer: A

Google explicitly recommend A:

https://developers.google.com/admin-sdk/admin-settings/limits

upvoted 4 times

cloudguy2 11 months, 3 weeks ago

correct answer is A - https://developers.google.com/admin-sdk/admin-settings/limits - B is not correct as directory api is not in scope for domain-wide delegation api

upvoted 2 times

ryuhei 1 year, 1 month ago

Selected Answer: A

Answer is "A" maybe

upvoted 1 times

nhiguchi 1 year, 1 month ago

Selected Answer: A

A 503 error response indicates a temporary problem that will likely be resolved by retrying after a period of time. Exponential backoff will help in this case because it is an efficient way to retry while allowing time for the temporary problem to be resolved.

upvoted 2 times

[Removed] 1 year, 1 month ago

Selected Answer: B

this option isnt complicated. it's the google way

upvoted 2 times

klu23 1 year, 1 month ago

Selected Answer: C

https://developers.google.com/admin-sdk/directory/v1/guides/troubleshoot-error-codes

C should solve the problem

upvoted 1 times

Cert1Magic2 10 months, 3 weeks ago

Why you feel that sending 1000 of request in a batch will not create the same issue? Better solution will be to go for exponential backoff retry which works as "Exponential backoff is an algorithm that uses feedback to multiplicatively decrease the rate of some process, in order to gradually find an acceptable rate. These algorithms find usage in a wide range of systems and processes, with radio networks and computer networks being particularly notable."

upvoted 1 times

zzzzzooooo 1 year, 1 month ago

Selected Answer: A

I geuss A

upvoted 1 times

Question #56 *Topic 1*

A user does not follow their sign-in pattern and signs in from an unusual location. As an admin, what should you do in response to this alert for this user during this investigation?

A. Add Two Factor Authentication to the Domain

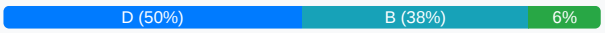
B. First, suspend the account and then investigate

C. Enhance your security alerts for tracking sign-in patterns

D. Investigate the account for unauthorized activity in the Login and Security Audit Log

Suggested Answer: *B*

Community vote distribution



csavar 2 weeks, 5 days ago

or B

google said, always suspend first in the docs

upvoted 1 times

JessiePiper 3 months, 3 weeks ago

Selected Answer: B

I agree with B here. In this specific instance, where you've already confirmed suspicious activity and an unusual login location, the logs wouldn't provide any additional information that would change your immediate course of action. I think you are still missing some steps in between, but B makes the most sense to me.

upvoted 1 times

Nico282 8 months, 4 weeks ago

Selected Answer: B

I was going with the sensible choice to investigate on the logs, but as there is no "Login and Security Audit Log" in the admin console, I believe that "Suspend first" is the answer Google wants in this scenario: https://support.google.com/a/answer/2984349?hl=en

Personally I wouldn't suspend the CEO account on a business trip before checking for additional clues.

upvoted 3 times

examprof 9 months ago

Option B. Please follow me:

This link includes precisely the scenario described here ("user does not follow their sign-in pattern and signs in from an unusual location") as an example of suspicion login:

https://support.google.com/a/answer/7102416?hl=en

As a first step, it instructs the admin to "Ask the user with the suspicious login if they remember signing in", which is not included as a possible answer in the alternatives.

Then, as a second step, it instructs admin to "follow the Administrator security checklist", which may be found here:

https://support.google.com/a/answer/2984349?hl=en

The very first step is "SUSPEND a user to prevent unauthorized access." followed by "Investigate the potentially unauthorized activity...".

At last, there's no such thing named "Login and Security Audit Log" in Google Workspace (not with this name).

I vote for Option B. Suspend first, investigate after.

upvoted 4 times

virat_kohli 10 months, 2 weeks ago

Selected Answer: D

D. Investigate the account for unauthorized activity in the Login and Security Audit Log

upvoted 1 times

jcloud965 10 months, 2 weeks ago

Selected Answer: B

Answer is B. Identifying and securing compromised accounts should start by temporarily suspending the suspected compromised user account to prevent unauthorized access, then investigating the potentially unauthorized activity and finally restoring the account. https://support.google.com/a/answer/7102416?hl=en

Answer D : We already know that user signed in from an unusual location. Login Audit Log will provide the unsual IP address only. There is no "Security Audit Log" in the admin console.

upvoted 2 times

jcloud965 10 months, 2 weeks ago

Selected Answer: C

Answer is C. Identifying and securing compromised accounts should start by temporarily suspending the suspected compromised user account to prevent unauthorized access, then investigating the potentially unauthorized activity and finally restoring the account. https://support.google.com/a/answer/7102416?hl=en

Answer D : We already know that user signed in from an unusual location. Login Audit Log will provide the unsual IP address only. There is no "Security Audit Log" in the admin console.

upvoted 1 times

zanhsieh 11 months, 3 weeks ago

Selected Answer: D

Vote D. Remember we need to have the root cause analysis, then decide which action would take.

A: No. Adding 2FA is one of the following-up actions.

B: No. Suppose a CxO logging into the domain in the customer site just for the meeting (he obviously won't tell Workspace admin his schedule), of course Workspace admin won't suspend the CxO access immediately.

C: No. Again, this is the following-up action.

D: Yes. Knowing the root cause is the first step to take.

upvoted 2 times

ryuhei 1 year, 1 month ago

Selected Answer: D

Answer is D

upvoted 1 times

[Removed] 1 year, 1 month ago

Selected Answer: D

D for sure

upvoted 1 times

wborquez 1 year, 1 month ago

Selected Answer: D

D is the correct

upvoted 1 times

Jane1234YIP 1 year, 1 month ago

Selected Answer: D

D is the correct Answer!

upvoted 1 times

klu23 1 year, 1 month ago

Selected Answer: D

D seems legit

upvoted 1 times

Prosecute 1 year, 1 month ago