Boost up Your Certification Score

SAP
C_SEC
SAP Certified - Security Administrator

For More Information – Visit link below:

https://www.examsboost.com/

Product Version

✓ Up to Date products, reliable and verified.
✓ Questions and Answers in PDF Format.

Visit us at: https://www.examsboost.com/test/c-sec

Latest Version: 4.0

1. Micro Skill Drill Exam
2. Unified Scenario Exam

Topic: 1
Micro Skill Drill Exam

Question: 1

A regional newspaper uses SAP Cloud Identity Services, where employees already sign in to its existing cloud applications with single sign-on through the Identity Authentication Service. The newspaper has just adopted an additional SAP cloud application for its advertising team, and the team wants employees to reach it with the same single sign-on they already use for the other apps, rather than having to remember and maintain a separate password just for the new one. Keeping one consistent sign-in also means fewer help-desk password resets and one place to manage how people authenticate. The administrator must set the new application up so that it relies on the authentication employees already have, keeping the sign-in experience consistent across the whole landscape rather than introducing yet another separate login just for this one new app.
What is the correct way to give employees single sign-on to the new application?
Response:

A. Have employees set up a separate local password for the new application, since each cloud application is expected to manage its own sign-in on its own.
B. Assign each employee a launchpad business catalog for the new app, because the catalog is what enables single sign-on to a cloud application.
C. Connect the new application to the existing Identity Authentication Service, so it uses the single sign-on employees already have.
D. Set up a second, separate identity service dedicated to the new application, so its sign-in is kept independent from the existing applications.

Answer: C

Explanation:
Feedback:
Employees already authenticate to the existing apps through the Identity Authentication Service, so connecting the new application to that same service lets them reach it with the single sign-on they already use. This delivers a consistent sign-in across the landscape and avoids a separate password, which is exactly what the team wants. It extends the existing authentication to the new app.

Question: 2

A semiconductor manufacturer runs on-premise SAP S/4HANA across several fabrication sites. To keep authorizations consistent, it maintains one central master role for fab technicians and a set of site-specific roles derived from it: each derived role inherits the master's authorizations but carries its own

site's organizational values. Last week the security team added a new authorization to the master role for a new quality-logging function. Technicians at one site still cannot use the function and receive an authorization error. The administrator checks carefully: the master role now contains the new authorization, the technician's derived role for that site is assigned and active, and his organizational values are correct for the site. The gap is that after the master changed, the derived roles were never regenerated to pull the new authorization down, so the derived role the technician actually holds still reflects the master as it was before the change. Company practice requires derived roles to be regenerated from the master whenever the master's authorizations change. The team's first instinct, since the master clearly carries the authorization, is to open the master and add it again. The administrator must work out why the derived role lags behind and correct it properly.
Why can the technician not use the function, and what is the correct action?
Response:

A. His organizational values are wrong for the site, so correct the values held on the derived role and the new quality-logging function will then work for him.
B. The derived roles were not regenerated after the master changed; regenerate them so they inherit the new authorization.
C. Add the new authorization directly onto the technician's user record, separately from the role, so that he is able to use the function right away.
D. Open the master role and add the authorization again, since the change evidently failed to save into the master role properly the first time.

Answer: B

Explanation:
Feedback:
Derived roles inherit their authorizations from the master, and the master gained the new authorization but the derived roles were never regenerated to take it in, so the technician's derived role still carries the pre-change content. Regenerating the derived roles from the master pulls the new authorization into the role he actually holds, which makes the quality-logging function work while preserving each site's own organizational values. This corrects the lag at the right level.

Question: 3

A textile dyer running on-premise SAP S/4HANA finds during an access review that a lab technician can reach purchasing functions she should not have. The administrator checks her directly assigned roles and finds nothing that grants purchasing — her direct roles are all lab-related and entirely appropriate to her job. The extra access comes from elsewhere: the dyer assigns some roles indirectly through positions in its organizational structure, and the position the technician was recently moved into still carries a purchasing role left over from the responsibilities of its previous holder. So her direct roles are clean, but an indirect role assignment through her position is what grants the purchasing access. The dyer follows least-privilege and expects each person's access to match their actual duties, with nothing carried over from a position's previous holder. The team's first instinct, having confirmed her direct roles are appropriate, is to conclude there is nothing wrong. The administrator must remove the purchasing access the technician should not have, at the point where it is actually coming from.
Why does the technician have purchasing access, and what is the correct action?
Response:

A. Conclude there is no issue to fix, since the technician's directly assigned roles are all appropriate and none of them grants any purchasing access.
B. Remove the purchasing role from the position the technician now holds, since it is granting that access indirectly and no longer fits the position.
C. Remove all of the technician's direct roles and rebuild them, since the unexpected purchasing access means her direct role assignment must be wrong.
D. Add a restriction on her user that blocks purchasing, leaving the position's purchasing role in place for whoever holds the position next.

Answer: B

Explanation:
Feedback:
Her direct roles grant no purchasing, so the access must come from the indirect assignment through her position, which still carries a purchasing role from its previous holder. Removing that purchasing role from the position stops the indirect grant at its source and also corrects the position for whoever holds it next, since it no longer fits the role. This fixes the access exactly where it originates.

Question: 4

A pharmaceutical manufacturer is rolling out SAP Fiori apps to replace classic transaction screens on its on-premise SAP S/4HANA system, and during the cut-over both interfaces remain available to users. During this coexistence period, a quality reviewer can still complete the equivalent task in the classic SAP GUI without issue. However, when she opens the new Fiori app from the launchpad, the tile is visible but the app returns an error and shows no dat
a. The administrator works through what is in place: the reviewer's role grants the underlying authorization objects that the classic transaction uses, and the Fiori tile appears because the business catalog for the app is included in her role. A second reviewer, working from a different role, opens the same Fiori app and sees the data normally, which tells the administrator the app itself is configured correctly. Because the tile is present, the classic transaction works, and a colleague's app loads fine, the team's first instinct is that the reviewer's catalog assignment must somehow be incomplete and should be reapplied to clear the data error.
What is the most likely cause of the failure, and what is the correct corrective action?
Response:
A. The app's business catalog is missing from her role, so add the catalog to her role again and both the tile and the app's data will then load correctly for her.
B. The backend authorization the app checks is missing from her role even though the launchpad catalog is present; grant that missing authorization.
C. The classic transaction authorization is conflicting with the new Fiori app, so remove the classic authorization from her role and the app will stop returning the error.
D. The launchpad needs to be reactivated for her user so that the visible tile resolves to the correct app and begins returning the expected data again.

Answer: C

Explanation:
Feedback:
A Fiori app needs both frontend authorization (the catalog that shows the tile) and the backend authorization the app checks when it reads data. Here the tile shows, so the frontend side is in place, but the app errors with no data, which points to the backend service authorization the app requires being absent from her role. The working reviewer's different role evidently includes that backend authorization. Granting the missing backend authorization aligns both layers and resolves the root cause rather than the visible symptom.

Question: 5

A commercial laundry running on-premise SAP S/4HANA has a route planner who is blocked when she opens a delivery-planning transaction: it fails with an authorization error immediately, before she has entered anything. Oddly, if she then manually changes the plant shown at the start to her own depot's plant, the transaction works normally from that point on. The administrator confirms her role authorizes the planning transaction for her own depot's plant, and only that plant. Looking at her user settings, the administrator finds a personal default value stored on her account that pre-fills a different plant — one belonging to a depot she transferred away from some time ago. When she opens the transaction it starts on that pre-filled plant, which she is no longer authorized for, so it fails on the spot; changing it to her current plant is what lets it through. Her role is correct for the depot she now serves; the stale personal default is what triggers the failure at startup. The laundry follows least-privilege and scopes each planner to their own depot. The team's first instinct, seeing an authorization error, is to widen her plant authorization. The team has confirmed her role is correct for her current plant and that overriding the pre-filled plant makes the transaction work, but has not yet pinned down why it fails the instant she opens it.
What is the most likely cause of the startup failure, and the correct action?
Response:

A. Grant her plant authorization for the depot the transaction starts on, so that it stops failing at the moment she opens it.
B. Tell her to change the plant manually each time she opens the transaction, since doing that already makes it work for her.
C. Update the stale personal default on her user to her current plant, so it opens on a plant she is authorized for.
D. Recreate her user to clear whatever causes the startup failure, then reassign her planning role afterward.

Answer: C

Explanation:
Feedback:
A personal default value on her user pre-fills a plant she is no longer authorized for, so the transaction starts on it and fails immediately, while overriding it to her current plant works — which points squarely at the stale default. Updating that default to her current plant makes the transaction open on a plant she is authorized for, removing the startup failure without changing any access. This corrects the actual trigger.

Question: 6

A national bakery chain running on-premise SAP S/4HANA is onboarding a new production scheduler who will do the same job as several existing schedulers on the team. She starts next week on the same shift pattern and the same plants as her peers, so her access needs are well understood from theirs. The chain maintains a standard role for the production-scheduler position — the existing schedulers already hold it, and it grants exactly the access the job requires and nothing more. The security team has been asked to avoid the bespoke, hand-assembled roles that crept in during past onboardings and later proved hard to audit. The administrator wants the new joiner's access to match her position and stay consistent with her peers, without creating one-off access that is awkward to maintain later. Company practice is to provision new staff with the standard role defined for their position.
What is the correct way to provision the new scheduler's access?
Response:

A. Build a new custom role just for her by copying pieces of access from several colleagues until she can do the job.
B. Grant her broad access now so she is not blocked on day one, then trim it down to what she actually needs at a later review.
C. Assign her the standard production-scheduler role her peers already hold, which grants exactly what the position requires.
D. Give her a manager-level role for now so she can self-select the functions she finds she needs as she learns the job.

Answer: C

Explanation:
Feedback:
The chain maintains a standard role for the production-scheduler position that her peers hold and that grants exactly what the job requires. Assigning her that role gives her precisely the access she needs, keeps her consistent with the team, and stays maintainable because the access is defined once in the shared role. This matches company practice and least-privilege.

Question: 7

A charity running SAP discovers that a volunteer who left several months ago still had an active account, and used it last week to sign in and download a file of supporter contact details. The access should have ended when the volunteer left, but no one removed it, and nothing in the charity's process prompted its removal. The immediate harm is that a person no longer associated with the charity reached supporter data and took a copy. Beyond this one account, the charity realises it has no reliable step that removes a person's access when they stop volunteering, so other dormant accounts may exist. The trustees want both the immediate situation handled and the underlying weakness closed, so that someone who leaves cannot retain access afterwards. The charity holds personal data on its supporters and is accountable for protecting it. The trustees are conscious that supporter trust depends on that data being handled properly, and that access is expected to end when a person's involvement does. The team must decide on the correct response and the change that prevents a recurrence.

Visit us at: https://www.examsboost.com/test/c-sec

What is the correct response to the incident and the change that prevents a recurrence?
Response:

A. Reset the passwords of all current volunteers, so the supporter data is secured against further access.
B. Limit how much supporter data a volunteer can download at once, so any future leak would be smaller in size.
C. Revoke the former volunteer's access immediately and ensure access is removed whenever a person leaves.
D. Begin monitoring the supporter data for further unusual downloads, so any repeat is noticed.

Answer: C

Explanation:
Feedback:
Revoking the former volunteer's access immediately ends the misuse, and ensuring access is removed whenever a person leaves closes the underlying gap that let the account persist, so departed people cannot retain access. It handles both the specific incident and its cause. This is the response and the preventive change the situation calls for.

Question: 8

An art museum uses SAP Cloud Identity Services for its cloud applications, where staff currently sign in with a username and password through the Identity Authentication Service, as they have since the apps went live. One application holds especially sensitive donor and acquisition records, and after a recent scare the museum's security policy now requires that access to that application be protected by more than a password alone — a second verification step at sign-in for the people who use it. Most other museum apps hold nothing so sensitive and remain fine on a password alone, so the new requirement should not be forced on everyone. The administrator needs to strengthen sign-in for that sensitive application specifically, without forcing the change on every other app where it is not required. The administrator is deciding how to meet the new requirement.
What is the correct way to strengthen sign-in for the sensitive application?
Response:

A. Tell the staff who use the application to choose longer, more complex passwords, since a stronger password removes the need for any second step.
B. Configure the authentication service to require an additional verification step at sign-in for the sensitive application, beyond the password.
C. Restrict which apps appear on each user's launchpad, on the basis that hiding the sensitive app from most people protects who can sign in to it.
D. Move the donor and acquisition records into a separate database, since storing them apart strengthens how users authenticate to the application.

Answer: B

Explanation:
Feedback:

The policy requires access to the sensitive application to be protected by more than a password, and the authentication service can require an additional verification step at sign-in for that specific application. Configuring it there adds the second factor exactly where it is needed, without imposing it on apps that do not require it. This meets the requirement precisely.

Question: 9

A dairy cooperative runs reporting on SAP HANA Cloud. A reporting developer can read and query all the data she needs in the analytics schema without any trouble, but when she tries to create a new calculation view to combine some of that data, the database refuses the action. The administrator confirms her access to read the underlying data is complete and working — every table and view she queries returns results — and that other developers who build views in the same schema can do so. Nothing about the data she is combining is off limits to her; she can already select all of it. The refusal comes only when she attempts to create the new object itself, not when she reads its inputs. Her grants were set up to let her consume the cooperative's data for reporting, and creating objects was not part of that original setup. The cooperative follows least-privilege. She can query everything she needs but cannot build the view, and she needs to be able to create it.
Why can the developer query the data but not create the view, and what is the correct action?
Response:

A. Grant her read access to additional schemas, since being unable to build the view suggests she is missing data the view needs.
B. Have her ask a developer who can build views to create it for her, since they already have that ability.
C. Re-grant her read access through a role instead of directly, since how her reads are granted may be what blocks creating the view.
D. Grant her the development privilege for creating database objects, alongside her existing read access.

Answer: C

Explanation:
Feedback:
Reading data and creating objects are governed by different kinds of privilege; her grants thoroughly cover reading but were never set up to allow creating objects, which is why she can query everything yet is refused when she builds the view. Granting her the development privilege for creating database objects, alongside the read access she already has, lets her build the view while staying scoped. This adds the precise capability that is missing.

Question: 10

A food-delivery platform requires an additional authentication factor at sign-in for a sensitive operations application, configured in the Identity Authentication Service. After rollout, most staff are prompted for the second factor when they open the app, but one team — the late-shift dispatchers — still get in with a password alone. The administrator establishes two things. First, the additional-factor requirement is correctly configured and enforced for the application in general, which is why most staff are prompted. Second, an authentication rule carries an exception that exempts the late-shift dispatchers' group from the second factor, left over from a pilot phase when that group was deliberately excluded and never re-

included afterward. So the requirement is on, but a standing exception lets one group bypass it. The platform's policy now requires the second factor for everyone who uses the application, with no exceptions. The team's first instinct, seeing the gap, is to re-apply the additional-factor requirement to the application. The administrator must close the bypass so the dispatchers are also challenged for the second factor.
Why do the dispatchers still get in with a password alone, and what is the correct action?
Response:

A. Remove the exception that exempts the late-shift dispatchers' group, so the additional-factor requirement applies to them too.
B. Re-apply the additional-factor requirement to the application, since one group still bypassing it shows the requirement did not fully take effect.
C. Tell the dispatchers to set stronger passwords, since a sufficiently strong password gives their shift adequate protection on its own.
D. Move the sensitive application behind a different launchpad for the dispatchers, so that their route into it enforces the second factor.

Answer: A

Explanation:
Feedback:
The requirement is correctly enforced for the application, and the dispatchers bypass it only because a leftover exception exempts their group. Removing that exception brings the group under the same additional-factor requirement as everyone else, which is exactly what the policy now demands. This fixes the actual cause — the standing exemption — rather than the requirement that already works.
Topic: 2
Unified Scenario Exam

Question: 11

CHALLENGE 1 — Setting Up Central Sign-In and Account Provisioning
The chain wants staff to sign in once centrally and have their accounts in connected applications created automatically.
Which capabilities of the central identity service meet these two needs?
Response:

A. Provisioning for sign-in, and authentication for creating the accounts.
B. Authentication for sign-in, provisioning for the accounts.
C. Authentication for both sign-in and creating the accounts.
D. Provisioning for both sign-in and creating the accounts.

Answer: B

Explanation:
Feedback:

Authentication proves who a user is at sign-in, and provisioning creates and manages their accounts in connected applications, so the two needs map to those two capabilities. Using authentication for sign-in and provisioning for the accounts meets both. Each capability does its own job.

Question: 12

CHALLENGE 1 — Setting Up Central Sign-In and Account Provisioning
A new joiner can sign in centrally, but one connected application does not recognize her.
What is the most likely cause and the correct action?
Response:

A. Her central sign-in is broken; set up her authentication again so the application accepts her.
B. The application is down for her; have her wait and try again later.
C. She has not yet been provisioned into that application; ensure provisioning to it completes.
D. She needs broad access in the application; grant it so she is recognized.

Answer: C

Explanation:
Feedback:
She can sign in, so authentication works; the application does not recognize her because her account has not yet been provisioned there. Ensuring provisioning to that application completes connects her to an account in it. The gap is the account setup, not sign-in.

Question: 13

CHALLENGE 1 — Setting Up Central Sign-In and Account Provisioning
The chain wants to stop setting up each application by hand for every new hire across its clubs.
What is the correct way to set up new joiners' access?
Response:

A. Provision accounts automatically from the central source, by each joiner's job.
B. Keep setting up each application by hand, but have one club do it for all the others.
C. Give every new joiner a shared club login so no per-person setup is needed.
D. Grant each joiner broad access on their first day and trim it later.

Answer: A

Explanation:
Feedback:
Provisioning accounts automatically from the central source, driven by each joiner's job, replaces the manual per-application setup with one consistent process across the clubs. It is fast and uniform. This is what the chain is trying to achieve.

Question: 14

CHALLENGE 1 — Setting Up Central Sign-In and Account Provisioning
A staff member has left the chain, and the team wants her access removed across the connected applications.
What is the correct way to handle this, now and in future?
Response:

A. Reset her password but leave her accounts in place in case she returns.
B. Reduce what her accounts can do, but keep them active for now.
C. Watch her accounts for any activity and act only if they are used.
D. Remove her accounts through provisioning once she is recorded as left.

Answer: D

Explanation:
Feedback:
Provisioning that removes accounts when the central record shows a person has left clears her access across the connected applications cleanly, and does so for everyone in future. A departed person should retain nothing. This closes the inconsistent-removal gap at its source.

Question: 15

CHALLENGE 2 — Protecting Members' Personal Data
A staff role reaches member personal data that the job does not actually need.
What is the correct action?
Response:

A. Leave the access, since the staff are trusted with member data anyway.
B. Give the same access to everyone, so it is at least consistent.
C. Scope the role to the personal data the job needs.
D. Hide the extra data on screen but leave the access in place behind it.

Answer: C

Explanation:
Feedback:
Personal data should be reachable only by staff whose job needs it, so scoping the role to what the job requires and removing the rest brings it within that principle. It keeps member data to those who need it. This is the correct, least-privilege fix.

Visit us at: https://www.examsboost.com/test/c-sec

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer