genbay
CORPORATE & ACADEMIC TRAINING

Enterprise IAM Lab
Practice questions

Answer key · instructor copy

Every question from the Genbay CIAM hands-on lab, with the validated solution beside it. Part A checks concepts, Part B is hands-on in the live lab, and Part C tests how the policy engine reasons. All Part B and Part C answers were executed against the running environment.

How to use this workbook

1. Hand candidates the **candidate edition** — same questions, answer space instead of solutions.
2. Part B expects the lab in its clean seeded state; reset it between candidates.
3. Part C is the fastest read of whether someone understands policy evaluation — watch C11/C12 (the threshold is **≤ 50,000**) and C14 (SoD denies *reads* too).
4. Solutions are deliberately short: they state the outcome *and* the reason, which is what the exam asks for.

Certified Identity & Access Manager
Hands-on lab · 7 IAM tools

29 questions
Part A · 7 Part B · 7 Part C · 15

mytrainingdocs.com
Delivered by Genbay

Part A — Concept checks

Exam-style. Place each tool and activity in the right category and Critical Risk Domain.

A1 CRD 3, 6

Which single tool is the *only* writer of the directory, and why is that rule so important?

SOLUTION

midPoint (IGA) is the only writer; Keycloak only *reads* the same directory. Because governance and authentication share one source of truth, a change in IGA — disabling a leaver, removing a role — instantly changes what the person can authenticate to and do, everywhere at once.

A2 CRD 8

A scenario describes running quarterly campaigns where managers confirm their team's access is still appropriate. Which tool category and CRD?

SOLUTION

IGA (midPoint), CRD **8 — Access Review & Re-Certification**. Reviews and certification live in the governance tool, not the login tool.

A3 CRD 6, 10

The Portal never stores a password. When a user visits it, how do they prove who they are, and what token / protocol is involved?

SOLUTION

The Portal redirects to **Keycloak** (the IdP), which authenticates the user (with MFA) and returns an **OIDC** token. The Portal trusts that token — it is an OIDC client / relying party. This is single sign-on.

A4 CRD 5, 6

Explain the difference between OPA and the Golonex Portal in one sentence each.

SOLUTION

OPA is the Policy *Decision* Point — it answers "is this allowed?" from policy-as-code. The **Portal** is the Policy *Enforcement* Point — it asks OPA before every action and enforces the answer.

A5 CRD 6, 7

The lab has two PAM-style tools. Name them and give one thing that distinguishes them.

SOLUTION

Teleport — identity-aware, just-in-time SSH with RBAC and mandatory MFA. **Guacamole** — a clientless gateway that also brokers RDP/VNC, entirely in the browser. Both *record* sessions.

A6 CRD 7

In the capstone, a terminated employee's login attempt triggers a SIEM alert. What is the underlying technical signal, and why does it occur?

SOLUTION

Keycloak records a `LOGIN_ERROR` with error `user_not_found`. After termination, midPoint disables the account and Keycloak's federation filter hides disabled accounts — so to Keycloak the username no longer resolves. Wazuh's rule fires on that as a "possible post-termination access attempt".

A7 CRD 1, 2

Which two Critical Risk Domains does this lab *not* perform hands-on, and why is that reasonable?

SOLUTION

CRD 1 — Strategy & Governance and **CRD 2 — Program Management**: planning and organisational disciplines rather than operational tasks. The lab assumes them and exercises the operational domains, CRD 3–10.

Part B — Hands-on exercises

Before you start

Seeded users (password `Welcome2026!`): `bob.builder` (IT), `carol.chen` (Finance manager / approver), `dave.dixon` (HR), `erin.evans` (AP clerk). Every solution below was run in the live lab.

B1 JOINER · CRD 3, 5

Onboard a new employee — **Priya Patel**, department **IT**, "Service Desk Analyst" — from the HR feed, and prove she can log in. What access does she get automatically, and why?

SOLUTION

Add Priya in the Portal HRIS; run midPoint's HR-import. Result (validated): she is created *enabled*, department IT, with the **Employee** birthright role → an OpenLDAP account and `app-users` membership. She logs into the Portal with `groups=[app-users]`. Baseline access is automatic because the birthright role is auto-assigned to every HR-sourced identity.

B2 REQUEST & APPROVAL · CRD 4

Grant Priya the **HR Staff** entitlement through the proper request path. Does it take effect immediately? Who must act?

SOLUTION

No — HR Staff is requestable, so it raises an **approval** routed to an *Access Approver* (a line manager). Only after approval does midPoint provision the `hr-staff` group. (It is also department-scoped, so it is only *effective* while the holder is in HR — the teaching point here is the approval routing.)

B3 SEGREGATION OF DUTIES · CRD 5, 6

erin.evans is an AP *clerk*. Try to *also* grant her the AP *Approver* role. What happens, and what is she left holding?

SOLUTION

The request is **blocked** — the roles are segregated (an SoD policy violation; HTTP 409 via the API). Erin keeps only `finance-ap-clerk`; the approver role is never granted. And OPA would deny all finance actions to anyone holding both.

B4 MOVER · CRD 3

Move a Finance AP clerk to the IT department in HR and re-run the import. What happens to their Finance entitlement, and why?

SOLUTION

The `finance-ap-clerk` entitlement is **automatically removed** — that role is scoped to Finance, so leaving Finance strips it; the directory group membership drops to baseline (`app-users`). This is how attribute-scoped roles prevent "access creep".

B5 RECONCILIATION · CRD 9

Run a directory reconciliation. One account is flagged as *unmatched*. Which one, and what makes it an orphan?

SOLUTION

mallory.mills. She exists in the directory but has **no owning identity in midPoint and no HR record** — created directly in the directory, bypassing governance. Reconciliation surfaces exactly these accounts. Validated: present in LDAP, no midPoint user.

B6 LEAVER + SOC · CRD 3, 6, 7

Off-board Priya (set status *terminated*, re-run import). Confirm she can no longer log in. Then attempt her old credentials and find the SIEM alert. What severity and message?

SOLUTION

She is disabled in midPoint, in the directory, and hidden from Keycloak — her Portal login fails. Attempting her old credentials produces, in **Wazuh**, a high-severity alert (**level 12**): *"login attempt for non-existent/disabled account … possible post-termination access attempt"*, with username, source IP and time.

B7 PRIVILEGED ACCESS · CRD 6, 7

Open a privileged session to a server through Teleport (or Guacamole), run a command, then locate the recording. What did you have to provide that a normal login does not require?

SOLUTION

MFA (a second factor for privileged access) and *just-in-time* access rather than a standing account. The session is **recorded** and replayable in the tool's UI. Accountability — who did what on which server, keystroke by keystroke — is the point of PAM.

Part C — Authorization challenges (OPA)

For each case, decide **ALLOW or DENY** — and why. The policy: everyone may view home; HR actions need `hr-staff`; invoice creation needs `finance-ap-clerk`; payment approval needs `finance-ap-approver`, and **above 50,000 also needs** `access-approvers`; admin needs `it-admins`; and holding *both* finance roles is a segregation-of-duties violation that denies all finance actions. All fifteen answers were validated against the live policy engine.

#	GROUPS THE USER HOLDS	ACTION (AMOUNT)	DECISION	WHY
C1	`app-users`	home.view	ALLOW	the home page is public to any signed-in user

#	GROUPS THE USER HOLDS	ACTION (AMOUNT)	DECISION	WHY
C2	`hr-staff`	hris.edit	ALLOW	HR edit requires `hr-staff` — held
C3	`hr-staff`	admin.view	DENY	missing entitlement (admin needs `it-admins`)
C4	`finance-ap-clerk`	invoice.create	ALLOW	invoice creation requires `finance-ap-clerk` — held
C5	`finance-ap-clerk`	payment.approve (100)	DENY	missing entitlement (approval needs `finance-ap-approver`)
C6	`finance-ap-approver`	payment.approve (5,000)	ALLOW	approver, amount ≤ 50,000
C7	`finance-ap-approver`	payment.approve (75,000)	DENY	amount above 50,000 requires a manager (`access-approvers`)
C8	`finance-ap-approver`, `access-approvers`	payment.approve (75,000)	ALLOW	approver + manager, so the large amount is permitted
C9	`finance-ap-clerk`, `finance-ap-approver`	invoice.create	DENY	SoD violation — holds both finance-ap-clerk and finance-ap-approver
C10	`it-admins`	admin.view	ALLOW	admin view requires `it-admins` — held
C11	`finance-ap-approver`	payment.approve (**exactly 50,000**)	ALLOW	boundary: exactly 50,000 is within the approver's limit
C12	`finance-ap-approver`	payment.approve (**50,001**)	DENY	boundary: 50,001 is above the limit → needs a manager
C13	*(none)*	home.view	ALLOW	home is public even with no groups
C14	`finance-ap-clerk`, `finance-ap-approver`	finance.view	DENY	SoD violation also blocks *reading* finance, not just writing
C15	`app-users`	invoice.create	DENY	a baseline user has no finance entitlement

Where candidates slip

C11 / C12 — the threshold is ≤ *50,000*, so exactly 50,000 passes and 50,001 does not. C14 — a segregation-of-duties violation denies *every* finance action, including read-only ones.