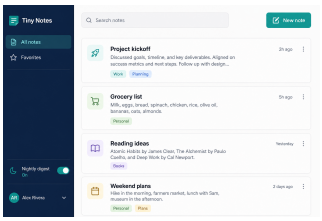
Tiny Notes Incident

You are on the team that runs Tiny Notes, an app for creating, editing, and searching notes.



Situation at 14:00

Tiny Notes uses a deployment service to update its production API. Its deployment token lets the team release new versions and roll back to earlier versions. The production API is working.

After a morning spent responding to a leaked deployment token, a teammate asks: “Can we close this incident and get back to the release?” You and a partner review the evidence below before answering.

ID	Evidence
E1	The old token was committed to a public repository at 09:00. A cleanup commit removed it from the file at 11:30.
E2	At 12:00, the team created a replacement token. A production deployment succeeded with it.
E3	The rollback job still uses the old token. A rollback test succeeded at 13:30.
E4	A secret scanner reports a possible credential in `tests/fixtures/fake_auth.json`. This test fixture contains a fixed value used only by a local test program that simulates checking credentials. The deployment service rejects the value.
E5	When `TINY_NOTES_DEPLOY_TOKEN` is missing, the deployment script uses a default value matching the old token. The latest secret scan reported only the finding in E4.
E6	The available access logs record requests to the deployment service from 11:30 onward. They show the team’s deployment using the replacement token and no unexplained requests. No logs are available for 09:00–11:30.

Your response

On the reverse of this sheet, write down your Andrew IDs and answer these questions.

1. What must happen first? Name two follow-up actions and anything you would do in parallel. Explain whether any action could interrupt the service or prevent deployments or rollbacks.
2. What evidence would you need to confirm containment and recovery? State what you still would not know.
3. Describe two example commits to test an automated secret-scanning check: one unsafe change it should block and one harmless change it should allow. For each example, name the file, describe its contents in words, and state the expected result.

Be ready to revise your examples when the instructor gives you new information.

Glossary

- **Credential:** A value used to prove identity when requesting access to a system, such as a password or token.
- **Deployment token:** A credential that lets a script or job request actions from the deployment service.
- **Production:** The running system that serves real users.
- **Rollback:** Replacing the current version with an earlier version.
- **Secret scanner:** A tool that searches files or Git history for possible credentials.
- **Test fixture:** Data or files prepared for use in a test.
- **Environment variable:** A named value supplied to a running program as configuration.
- **Containment:** Blocking the access exposed by the leak so it cannot be used to cause further harm.
- **Recovery:** Restoring and checking normal operation, including addressing any changes an attacker made.