

INTERNSHIP

CI/CD & Access Management

Automating pipelines for custom Keycloak extensions

Description of the assignment

This internship focuses on the continuous integration and deployment (CI/CD) of security fixes and version control for our access management product. This access management product is **Keycloak**. It's an open-source access management tool we implement and maintain for our clients, extended with a substantial set of custom-built plugins. Our infrastructure and deployment framework is built entirely with **Ansible**, so the pipeline you design will need to integrate smoothly into that ecosystem.

With the rise of AI-assisted vulnerability scanning, security issues are being identified faster than ever, which means new security fixes and Keycloak versions are released more frequently. Currently, whenever a new version becomes available, every custom extension must be manually verified to check whether it still builds correctly. Since we maintain **over 100 extensions**, this manual process is time-consuming and doesn't scale.

Your task is to **automate** this verification process by developing a **CI/CD pipeline** that covers all extensions. This while automatically testing and validating builds against new Keycloak releases and flagging any compatibility issues early. As part of this, the pipeline will also generate a **Software Bill of Materials (SBOM)** for each extension, giving us a clear, up-to-date inventory of every dependency in use. This makes it possible to instantly identify which extensions are affected when a new vulnerability is disclosed, rather than checking each one manually, and strengthens our overall compliance and audit posture.

This is a hands-on opportunity to work on a system that directly supports our clients and day-to-day operations. You'll gain practical experience with CI/CD design, Keycloak internals, infrastructure automation, and software supply chain security. All while making a real, measurable impact on how efficiently our team can deliver secure, up-to-date software.

Objectives

The goal of this internship is to design and implement an automated CI/CD pipeline that verifies the compatibility of 100+ custom Keycloak extensions with each new Keycloak release, while also strengthening our visibility into the software supply chain through automated SBOM generation. By replacing the current manual verification process, you will help the team respond faster and more reliably to security updates, reducing risk and freeing up engineering time for higher-value work.

Main objectives:

- **Automate build verification**
Develop a pipeline that automatically builds and tests all custom extensions against new Keycloak versions.
- **Detect compatibility issues early**
Implement checks that flag extensions which fail to build or behave unexpectedly with a new release, before deployment.
- **Generate SBOMs per extension**
Automatically produce a Software Bill of Materials for each extension during the build process, giving an up-to-date inventory of all dependencies in use.
- **Enable faster vulnerability response**
Use the generated SBOMs to quickly identify which extensions are affected when a new vulnerability is disclosed, instead of checking each one manually.
- **Integrate with existing infrastructure**
Ensure the pipeline works seamlessly within our Ansible-based deployment framework.
- **Ensure scalability**
Design the pipeline so it can easily extend to new extensions.
- **Document the process**
Provide clear documentation so the pipeline can be maintained and extended by the team after the internship ends.

Optional features

- **Robot Framework**
Beyond basic build verification, the pipeline will also incorporate functional testing using Robot Framework. This includes browser tests of the full authentication flow.
- **Static code analysis with SonarQube**
Scans extension source code for bugs, code smells, and security vulnerabilities before it's even built.

Technologies & concepts involved

✓	GitLab CI/CD	✓	Ansible
✓	Keycloak	✓	Docker
✓	Java	✓	Infrastructure as code
✓	SBOM	✓	Robot framework (extension)

Project Methodology

The project will follow a phase-based approach, allowing you to build a solid understanding of Keycloak and our existing infrastructure before gradually introducing automation. Here's a quick rundown of phases involved.

1. Onboarding & research

Get familiar with Keycloak's architecture, our custom extension codebase, and the existing Ansible-based deployment framework. Review the current manual verification process to understand pain points and edge cases firsthand.

2. Requirements & design

Define the scope of the pipeline together with the team: which build tools, CI/CD platform, and SBOM tooling to use, how the extension manifest will be maintained, and how the pipeline should integrate with the existing Ansible workflow.

3. POC (Proof of Concept)

Build a small-scale version of the pipeline covering a handful of extensions, to validate the approach (build automation, parallel execution, SBOM generation) before scaling up.

4. Implementation

Extend the proof of concept to cover all 100+ extensions. Implement parallel build execution, automated testing, SBOM generation, and vulnerability cross-referencing, integrating each step incrementally.

5. Testing & validation

Run the pipeline against real and historical Keycloak releases to validate accuracy and catch edge cases. Compare results against the previous manual process to confirm reliability.

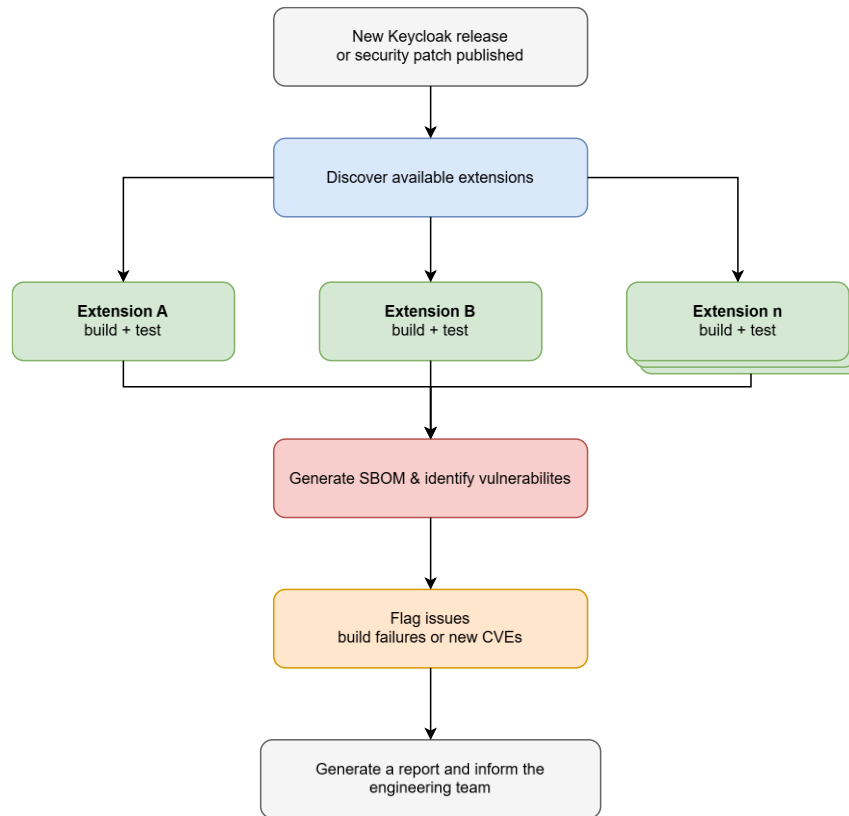
6. Documentation

Document the architecture, configuration, and maintenance procedures so the pipeline can be maintained and extended by the team after the internship ends.

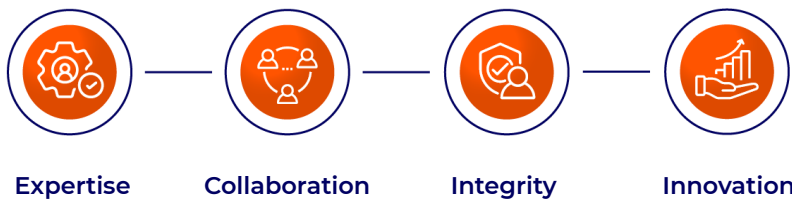
7. Evaluation

Gather feedback from the team, measure impact (time saved, issues caught earlier), and refine the pipeline based on real-world usage.

Overview



Profile



We are looking for a motivated student with an interest in Automation, Cybersecurity and IAM tools.

Preferred qualifications:

- Basic knowledge of ansible and Linux systems.
- Interest in automation and scripting.
- Familiarity with security concepts.
- Strong analytical and problem-solving skills.
- Ability to work independently while collaborating within a technical team.
- Eagerness to learn modern enterprise technologies and CI/CD practices.

Contact details

Contact person	Cindy Van den Hoecke	cindy.vandenhoecke@acen.eu
----------------	----------------------	----------------------------