

DevOps Specialist

Join the Team!

1 Introduction

The application procedure from tech11 has several steps. This test is one of it and gives us the opportunity to determine at which status you are regarding the necessary knowledge for this position.

Later on, if you succeed in this step, you will have the chance to present your solution within a personal interview (or remote via video chat). Here we will discuss your approach and have a deep dive into your solution/concept.

Please send your solution to jobs@tech11.com.

2 The Tasks

2.1 The DEV part

2.1.1 Hello World API Service

Please build a application in a programming language of your choice that provides a hello world REST endpoint.

The application should be packaged as Docker image.

2.1.2 Building

Please describe also a build pipeline for the *Hello World API Service*.

2.1.3 Say „Hello John“

Even if we say “Hello” to the world, the *Hello World API Service* shouldn’t be public.

The Hello World API Service must be protected. As Identity Access Management (IAM) tool we want to use Keycloak from RedHat (<https://www.keycloak.org>).

If you are more familiar with other IAM tools (also cloud based) you can use them instead of keycloak of course. But you should be able to implement the following requirements:

- Please setup a Docker network wherein the Hello World API Service and the IAM tool run (in case of a cloud based IAM tool, just link it together)
- Configure the *Hello World API Service* that he is protected by the IAM tool.
- Configure a user “john” with password “secret” within the IAM tool
- Extend the hello world endpoint that the return value is now “Hello <authenticated user>” (“Hello john”).

Now, the REST endpoint of *the Hello World API Service* should only be available by entering username and password.

Hint: For this test SSL is not required. In case you use keycloak: keycloak requires SSL per default – if you would like to keep it simple you can skip the SSL validation from keycloak by following this article: <https://stackoverflow.com/a/42002397/475834>

2.1.4 Say „Hello Social Media“

In a next step, please link the IAM tool to an OAUTH2 provider like github, google, linkedin, twitter or any other.

Extend the configuration at the IAM tool that the Hello World API Service is now also accessible by a user authenticated with one of the social auth provider.

2.2 The OPS part

At tech11 we use different cloud services like Office365, Jira or Bitbucket. At Hetzner (<https://hetzner.de>) we are hosting our dev and test servers (ssh access). Furthermore, our test applications, CI servers and the documentations are public available protected by username/password.

In detail we have:

- Microsoft cloud service (Office 365)
- Atlassian cloud service (Bitbucket, Jira)
- SSH access to our servers (only a few people)
- Web access to our applications / Jenkins / Sonar

You as the new DevOps specialist will be also responsible for maintaining user accounts.

Please describe your approach how to manage all the different credentials for all these services in a **pragmatic** way. Furthermore, please feel free also to rethink this stack.

Just describe your approach with some bullet points. We will discuss the details in a potential follow-up talk.

Please send the full project as zipped file to jobs@tech11.com.