Netzwerksicherheit, Praktikum

Prof. R. Zahoransky

Hochschule Furtwangen (University of Applied Science)

Aufgabe: Keycloak

Lernziel: IDM

Übersicht

Ziel dieser Aufgabe ist es, einen IdP zu konfigurieren Keycloak ist ein Open-Source-Identitätsanbieter. Keycloak bietet eine Benutzer-Föderation, starke Authentifizierung, Benutzerverwaltung, feingranulare Autorisierung und mehr.

Aufgabe 1: Setup

Ihnen wird wieder eine docker-compose Datei bereitgestellt, sodass Keycloak bereits startet. Nutzen Sie den Befehl `docker-compose up`.

Aufgabe:

- Auf welchem Port erreichen Sie die Keycloak-Oberfläche? Sehen Sie in der docker-compose Datei nach oder nutzen Sie den Befehl `netstat`.
- Gibt es ein Default-Passwort? Wie wird dieses Passwort an Keycloak gegeben?
- Erstelle ein Screenshot der Admin-Konsole

Aufgabe 2: User anlegen

Ein Realm ermöglicht es einem Administrator, isolierte Gruppen von Anwendungen und Benutzern zu erstellen. Zunächst umfasst Keycloak einen einzigen Bereich namens Master. Verwenden Sie diesen Bereich nur zur Verwaltung von Keycloak und nicht zur Verwaltung von Anwendungen.

Aufgabe:

- Erzeugen Sie ein Realm: **hfuBereich**
- Erzeugen Sie zwei Benutzer (userCM: Claudia Müller, cm@hfuBereich.de sowie userHM: Hans Meier, hm@hfuBereich.de).
- Erstelle ein Screenshot der Admin-Konsole. Darauf sollen die erstellen Benutzer zu sehen sein.
- Testen Sie den Login mit den neuen Usern und protokollieren Sie es. Die URL folgt der Form: `http://<Adresse>/realms/<realmname>/account`
- Hat der Login geklappt oder mussten Sie noch etwas weitere unternehmen?

Aufgabe 3: Konfiguration MFA

Konfigurieren Sie für einen User einen 2. Faktor für das Login

Aufgabe:

- Konfigurieren Sie OTP für einen User
- Zeigen Sie, dass es funktioniert.

Aufgabe 4: Anbindung eines Service Providers (SP)

Es soll ein Service per SAML als SSO angebunden werden. Einen Beispielservice ist bereits bereits in der docker-compose-Datei definiert: Nextcloud.
Im Internet finden Sie eine Vielzahl von Hilfestellungen. Mögliche Quellen, die Ihnen bei der Einrichtung helfen:

- https://stackoverflow.com/questions/48400812/sso-with-saml-keycloak-and-nextcloud
- https://janikvonrotz.ch/2020/04/21/configure-saml-authentication-for-nextcloud-with-keycloack/
- https://rmm.li/wiki/doku.php?id=linux_server_manuals:nextcloud_saml_authentication_against_keycloak
- https://rephlex.de/blog/2018/04/05/how-to-connect-nextcloud-to-active-directory-using-ad-fs-without-losing-your-mind/

Tipps:

- Unter dem Menüpunkt Realm Setting können Sie sich in Keycloak die Metadaten (XML-Datei) des IdPs ansehen. Darin finden Sie die Endpunkte und EntityID für Ihren Realm und Ihren IdP. Diese Informationen müssen Sie im Service Provider (Nextcloud) angeben.
- Sie können entweder openssl oder die Keycloak-Oberfläche zum Erstellen der Zertifikate nutzen

Aufgabe:

- Öffnen Sie die Nextcloud-Oberfläche. Erstellen Sie einen initialen Admin-Benutzer.
- Richten Sie **NICHT** die empfohlenen Apps ein. Vor allem Nextcloud Office führt zu mehreren Fehlermeldungen pro Sekunde, sodass Sie keine Log-Dateien mehr ansehen könnten.
- Installieren Sie die Erweiterung (App) SSO & SAML authentication
- Konfigurieren Sie keyclock für SAML
- Zeigen Sie, dass es funktioniert.

Optionale Zusatzaufgaben

- Sie können nun einen zweiten Dienst an Keycloak anbinden. Der Effekt ist, dass Sie sich nur einmalig anmelden müssen und nahtlos von einem zum anderen Dienst wechseln können, ohne erneut ein Passwort oder zweiten Faktor angeben zu müssen
- Sie können auch mit einer anderen Gruppe zusammenarbeiten und einen zweiten Keycloak-Server anbinden. Somit hätten „fremde“ Benutzer ebenfalls Zugriff auf Ihre Nextcloud Instanz.