



Abschlussprüfung Winter 2023

Fachinformatikerin für Systemintegration
Dokumentation zur betrieblichen Projektarbeit

Implementierung von MFA

**Implementierung von Multi-Faktor-Authentifizierung (MFA) zur
Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen
Services in einer Cloud-Infrastruktur**

Abgabetermin: Leipzig, den 10.11.2023

Prüfungsbewerber:

Melissa Futtig
Stephaniplatz 3
04317 Leipzig

Deloitte.

Ausbildungsbetrieb:

DELOITTE Wirtschaftsprüfungsgesellschaft GmbH

Dittrichring 22
04109 Leipzig

Winterprüfung 2023

Ausbildungsberuf

Fachinformatiker/Fachinformatikerin (VO 2020) Fachrichtung: Systemintegration

Prüfungsbezirk

Leipzig FISY 1 (AP T2V1)

Melissa Futtig

Identnummer: 886355

Prüflingsnummer: 52065

E-Mail: mfuttig@deloitte.de, Telefon: +49 1575283 33896

Ausbbildungsbetrieb: Deloitte GmbH Wirtschaftsprüfungsgesellschaft

Projektbetreuer: Edgar Kapler

E-Mail: ekapler@deloitte.de, Telefon: +49 1515448 4702

Thema der Projektarbeit

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

1 Thema der Projektarbeit

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

2 Geplanter Bearbeitungszeitraum

Beginn: 30.10.2023

Ende: 10.11.2023

3 Ausgangssituation

In der Deloitte Wirtschaftsprüfungsgesellschaft GmbH wird die Sicherheit des Zugriffs auf verschiedene Dienste innerhalb einer Cloud-Infrastruktur verbessert, indem Multi-Faktor-Authentifizierung (MFA) eingeführt wird. Dies geschieht, um eine erhöhte Sicherheit für firmeninterne und kundenbezogene Daten zu gewährleisten.

Ist-Analyse

Die Deloitte Wirtschaftsprüfungsgesellschaft GmbH verwendet die Cloud-Infrastruktur von OVHcloud, um einen Business Hosting Service bereitzustellen.

In dieser Konfiguration wird der Firewall eine öffentliche IP-Adresse zugewiesen. Das private Netzwerk enthält alle anderen Services und Instanzen und wird von der Firewall geschützt.

Eine Kontrollinstanz, namens „control_node“, ermöglicht den Zugriff auf alle anderen Instanzen, die sich im privaten Netzwerk befinden.

Die Cloud-Infrastruktur ist in vier Hauptbereiche unterteilt, in denen verschiedene Services/Dienste bereitgestellt werden:

A) Compliance and Security Stack

- Bereich für Compliance und Sicherheit
- Hierzu gehören eine OPNsense Firewall, ein Nginx Proxy Manager, der als reverse Proxy für das HTTP-Protokoll dient und andere Ports als Stream weiterleitet, der Guacamole Server und das Open-Source-Sicherheitstesttool Infection Monkey

B) Monitoring

- Überwachungsbereich aller vorhandenen Dienste der Cloud-Infrastruktur
- Beinhaltet die Open-Source-Software Grafana, Uptime Kuma als Webserver und Healchecks

C) DevOps

- Bereich für die Entwicklung und Bereitstellung von Anwendungen
- Enthält die kollaborative Entwicklungsplattform Gitlab, Nexus zur Verwaltung von Repositories, Sonarqube für die statische Analyse und Bewertung von Quelltextqualität, sowie

SFTPGO für die Authentifizierung mit öffentlichen Schlüsseln, SSH-Schlüsseln und Passwörtern

D) E-Mail

- E-Mail-Bereich
- Umfasst den Mail-Server Mailcow und SOGO für die E-Mail-Kommunikation

Der Zugriff auf die o.g. Dienste erfolgt durch die Eingabe eines Nutzernamens und eines Passworts. Dies erzeugt eine potenzielle Sicherheitslücke und macht die Dienste unserer Cloud-Infrastruktur anfälliger für Phishing-Angriffe und unbefugten Zugriff.

Soll-Konzept

Durch die Implementierung des MFA in der Cloud-Infrastruktur bei der Deloitte Wirtschaftsprüfungsgesellschaft GmbH soll durch das Hinzufügen einer weiteren Sicherheitsebene, Datenschutz und Integrität gewährleistet werden.

Die Deloitte Wirtschaftsprüfungsgesellschaft GmbH kann in alle Cloud-Services MFA integrieren, sodass durch dieses eine zusätzliche Sicherheitsebene aktiviert wird.

Vorgang:

Zu Beginn erfolgt die Passworteingabe des Nutzers. Unter der Voraussetzung der Korrektheit, erhält dieser einen Sicherheitscode per SMS, E-Mail oder einer App, welcher eingegeben wird und zu einer erfolgreichen Anmeldung führt.

Mehrere fehlgeschlagene MFA-Versuche führen zu einer Sperrung des Kontos oder erfordern eine Rücksetzung durch den Administrator.

4 Projektziel

Das Hauptziel des Projekts besteht darin, die Sicherheit der Cloud-Infrastruktur der Deloitte Wirtschaftsprüfungsgesellschaft GmbH bei der Zugriffskontrolle auf die o.g. Services zu erhöhen, indem Multi-Faktor-Authentifizierung (MFA) eingeführt wird.

Dabei steht im Vordergrund das Ziel der Risikominimierung durch die Einführung einer zusätzlichen Authentifizierungsebene. Nur unter der Voraussetzung des zweiten Faktors kann eine erfolgreiche Anmeldung erfolgen.

Um die Arbeitsabläufe der Mitarbeiter nicht zu beeinträchtigen, wird darauf geachtet, die Benutzerfreundlichkeit aufrechtzuerhalten und die MFA-Lösung darauf zugeschnitten.

Die technische Umsetzung von Sitecars (Single Sign-On with Integrated Credential and Authentication System) für MFA ist eine effektive Methode, um die Sicherheit von Zugriffskontrollen auf verschiedene Services in unserer Cloud-Infrastruktur zu verbessern.

Diese Methode ermöglicht eine zentrale Verwaltung von Benutzeranmeldungen und -authentifizierung, wobei MFA eine zusätzliche Sicherheitsebene hinzufügt. Die Implementierung erfolgt in Docker-Container und ermöglicht eine einfache Bereitstellung und Portabilität zwischen verschiedenen Umgebungen.

Folgende Kriterien sollen erfüllt werden:

A) IT-Sicherheit

- Minimierung von Risiken, wie Passwort-Leaks und Phishing
- Anmeldung ist nur mit MFA möglich

B) Reibungsloser Benutzerzugriff

- Nutzerauthentifizierung, um Zugriff auf die o.g. Services zu erhalten
- Anmeldung/ Sperrung des Nutzers

C) Compliance

- Erfüllung von Sicherheits- und Datenschutzstandards

5 Zeitplanung

Planungsphase 5h

- Erstellen einer Ist-Analyse
- Erstellen einer Soll-Analyse
- Kostenplanung
- Projektumfeld
- Kosten- und Nutzanalyse
- Gantt-Diagramm
- Klärung der Projektziele

Implementierungsphase 14h

- Auswahl einer MFA-Lösung
- Installation und Konfiguration von Sitecars
- Konfiguration der MFA
- Integration mit Cloud-Diensten

Testphase 6h

- Überwachung der Laufzeit der Services
- Überprüfung/ Beseitigen von Fehlern
- Zugriffstests

Einführung und Übergabe 4h

- Ausführung und Ergebnisübergabe
- Schulung der zu Beteiligten für die Nutzung

Dokumentation 6h

- Erstellung einer Projektdokumentation der Ergebnisse
- Erstellung einer Entwicklerdokumentation

Gesamt: 35h

6 Anlagen

keine

7 Präsentationsmittel

- Laptop
- Beamer
- 5 Ausdrucke der Präsentation für den Notfall
- Ladekabel Laptop
- HDMI-Kabel
- USB-C Kabel
- PowerPoint

8 Hinweis!

Ich bestätige, dass der Projektantrag dem Ausbildungsbetrieb vorgelegt und vom Ausbildenden genehmigt wurde. Der Projektantrag enthält keine Betriebsgeheimnisse. Soweit diese für die Antragstellung notwendig sind, wurden nach Rücksprache mit dem Ausbildenden die entsprechenden Stellen unkenntlich gemacht.

Mit dem Absenden des Projektantrages bestätige ich weiterhin, dass der Antrag eigenständig von mir angefertigt wurde. Ferner sichere ich zu, dass im Projektantrag personenbezogene Daten (d. h. Daten über die eine Person identifizierbar oder bestimmbar ist) nur verwendet werden, wenn die betroffene Person hierin eingewilligt hat.

Bei meiner ersten Anmeldung im Online-Portal wurde ich darauf hingewiesen, dass meine Arbeit bei Täuschungshandlungen bzw. Ordnungsverstößen mit „null“ Punkten bewertet werden kann. Ich bin weiter darüber aufgeklärt worden, dass dies auch dann gilt, wenn festgestellt wird, dass meine Arbeit im Ganzen oder zu Teilen mit der eines anderen Prüfungsteilnehmers übereinstimmt. Es ist mir bewusst, dass Kontrollen durchgeführt werden.

9 Grund für „mit Auflage genehmigt“

Guten Tag Melissa Futtig,
bitte achten Sie darauf, dass Ihre "Projektdokumentation der Ergebnisse" auch die Projektarbeit für den Prüfungsausschuss wiederspiegelt. In der Fachrichtung Systemintegration wird keine Entwicklerdokumentation erwartet, aber eine Kunden- und/oder Benutzerdokumentation (siehe



Handreichung der IHK <https://www.leipzig.ihk.de/mb-04-112/>). Unglücklich ist die "Klärung der Projektziele" am Ende der Planung. Berücksichtigen Sie gegebenenfalls, dass Ihnen nach neuer Verordnung 40 Stunden für die Projektarbeit zur Verfügung stehen.

mit Auflage genehmigt

*Inhaltsverzeichnis***Inhaltsverzeichnis**

Abbildungsverzeichnis	IV
Tabellenverzeichnis	V
Listings	VI
Abkürzungsverzeichnis	VII
1 Einleitung	1
1.1 Projektumfeld	1
1.2 Projektziel	1
1.3 Projektbegründung	1
1.4 Projektschnittstellen	2
1.4.1 Technisch	2
1.4.2 Organisatorisch	3
1.4.3 Personell	3
2 Projektplanung	4
2.1 Projektphasen	4
2.2 Abweichungen vom Projektantrag	4
2.3 Ressourcenplanung	5
2.3.1 Sachmittelplanung	5
2.3.2 Personalplanung	5
2.3.3 Ablaufplanung und Meilensteine	6
2.4 Entwicklungsprozess	6
2.5 Anforderungsanalyse	6
2.5.1 Funktional	6
2.5.2 Nicht-Funktional	7
3 Analysephase	7
3.1 Ist-Analyse	7
3.2 Soll-Analyse	7
3.3 Wirtschaftlichkeitsanalyse	8
3.3.1 „Make or Buy“-Entscheidung	8
3.3.2 Projektkosten	8
3.3.3 Amortisationsdauer	9
3.4 Nicht-monetärer Nutzen	9
3.5 Anwendungsfälle	10
4 Entwurfsphase	10
4.1 Zielplattform	10

Inhaltsverzeichnis

4.2	Authentifizierungs-Tool	10
4.3	Geschäftslogik	11
4.4	Maßnahmen zur Qualitätssicherung	12
4.4.1	Produktorientierte Maßnahmen	12
4.4.2	Prozessorientierte Maßnahmen	12
5	Projektdurchführung	12
5.1	Vorbereitung der Entwicklungsumgebung	12
5.2	Auswahl einer MFA-Lösung	12
5.3	Erstellung der docker-compose.yml, .env	13
5.4	Konfiguration des NGinx Reverse Proxy Managers	14
5.5	Konfiguration von Authentik	14
5.6	Integration mit Cloud-Diensten	15
5.7	Konfiguration des zweiten Faktors	15
6	Testphase	15
6.1	Überwachung der Laufzeit der Services	15
6.2	Überprüfung/ Beseitigung von Fehlern	16
6.3	Zugriffstests	16
7	Dokumentation	16
7.1	Benutzerdokumentation	16
8	Fazit	16
8.1	Soll-/Ist-Vergleich	16
8.2	Lessons Learned	17
8.3	Ausblick	17
Literaturverzeichnis		18
Eidesstattliche Erklärung		19
A	Anhang	i
A.1	Gantt-Diagramm und Meilensteine	i
A.2	Detaillierte Zeitplanung	ii
A.3	Use Case-Diagramm	iii
A.4	Sequenzdiagramm CLI Zugriff auf die Instanzen	iv
A.5	Cloud-Infrastruktur	iv
A.6	docker-compose.yml	vi
A.7	.env	viii
A.8	Proxy Host Konfiguration	ix
A.9	Authentik Konfiguration	xi
A.10	NGinx Konfiguration	xii

Inhaltsverzeichnis

A.11	TOTP-Konfiguration	xiii
A.12	Benutzerdokumentation	xiii

Abbildungsverzeichnis

1	Use Case-Diagramm	iii
---	-----------------------------	-----

Tabellenverzeichnis

1	Zeitplanung	4
2	Personalplanung	5
3	Kostenaufstellung	9
4	Entscheidungsmatrix	11
5	Nutzwertanalyse zur MFA-Lösung	13
6	Soll-/Ist-Vergleich	17

Listings

Listings

Abkürzungsverzeichnis

Abkürzungsverzeichnis

TOTP Time-based One-time Password

1 Einleitung

1 Einleitung

1.1 Projektumfeld

Die Deloitte Wirtschaftsprüfungsgesellschaft GmbH ist ein internationales Unternehmen für Wirtschaftsprüfung, Steuer-, Unternehmens-, Risiko- und Finanzberatung. Die Deloitte hat Niederlassungen in vielen Ländern, darunter auch Deutschland. Mit Vertreter/-innen in über 150 Ländern weltweit und 415.000 Mitarbeiter/-innen bietet das Unternehmen eine breite Palette von Dienstleistungen für Unternehmen und Organisationen in verschiedenen Branchen. Im B&TCL, auch dem Business & Technology Center Leipzig, erbringt die Deloitte GmbH mit ihren 100 Mitarbeiter/-innen eine Vielfalt an Business Services, mit und ohne IT-Bezug und treibt Transformationsprojekte rund um die Themen Cyber Security, Digitalisierung, Prozessoptimierung oder Automatisierung voran.

Das Projekt ist ein Tochterprojekt eines größeren und beinhaltet die Implementierung eines Teilfeatures, was zur Verbesserung des Gesamtprojektes führt. In diesem arbeiten interne Mitarbeiter/-innen aktiv mit, um die Entwicklung des Projektes voranzutreiben. Dabei stellen diese die Zielgruppe dar.

1.2 Projektziel

Die Deloitte Wirtschaftsprüfungsgesellschaft GmbH verwendet die Cloud-Infrastruktur von OVH-Cloud, um einen Business Hosting Service bereitzustellen.

Ziel ist es, die Sicherheit des Zugriffs auf verschiedene Dienste innerhalb dieser Cloud-Infrastruktur zu verbessern, indem Multi-Faktor-Authentifizierung (MFA) eingeführt wird. Dadurch soll eine erhöhte Sicherheit für firmeninterne und kundenbezogene Daten gewährleistet werden, indem nur eine Anmeldung mit MFA möglich ist und resultierend daraus Risiken, wie Passwork-Leaks und Phishing vermieden werden können. Um das Ziel zu erreichen wird Authentik für die Implementierung von MFA auf verschiedene Services in der Cloud-Infrastruktur eingeführt. Dabei ist Authentik ein Open-Source-Identitätsanbieter (Identity Provider), der den Zugriff auf verschiedene Dienste und Ressourcen in der Cloud-Infrastruktur verwalten und sichern soll und legt den Fokus auf die Flexibilität und Vielseitigkeit.

1.3 Projektbegründung

Die Implementierung der MFA steigert die Sicherheit und gewährleistet, dass der Zugang zu Diensten und Daten in der Cloud-Infrastruktur nicht allein durch den Diebstahl eines Passworts gefährdet ist. Benutzer/-innen müssen zusätzlich zur Eingabe des Nutzernamens und Passworts einen weiteren Authentifizierungsfaktor, wie zum Beispiel ein Einmalpasswort, eingeben, was die Sicherheit erheblich erhöht. Dabei werden nicht nur firmeninterne und kundenbezogene Daten geschützt, sondern auch die Kundenzufriedenheit und das Vertrauen gegenüber der zukünftigen Kund/-innen erhöht. Dies hat hohe Priorität und verhindert unbefugten Zugriff auf sensible Informationen.

1 Einleitung

1.4 Projektschnittstellen

1.4.1 Technisch

Die in Kapitel 1.2 besagte Cloud-Infrastruktur wird in vier Hauptbereiche unterteilt, sodass in jedem dieser Bereiche verschiedene Services bzw. Dienste zur Verfügung werden.

Compliance and Security Stack

Dieser Bereich umfasst den Einsatz von Docker-Containern für Dienste, wie die OPNsense Firewall, den NGinx Proxy Manager, dem Authentik- und Guacamole Server und Infection Monkey zur Sicherheitsüberprüfung. Zusammenfassend ist zu sagen, dass der NGinx Proxy Manager als Reverse Proxy fungiert und den HTTP-Verkehr umleitet und andere Ports für Streaming-Anforderungen bedient. Der Guacamole Server dient als Proxy-Server und ermöglicht den Zugriff auf interne Dienste, die normalerweise nicht über eine Web-Schnittstelle erreichbar sind. Das Open-Source-Sicherheitstesttool Infection Monkey überprüft die Sicherheit der Infrastruktur. Mit dem Identitätsanbieter Authentik, werden verschiedene Identitäts- und Authentifizierungsmethoden in Anwendungen und Diensten ermöglicht, zu integrieren. Dadurch wird eine wichtige Schnittstelle für die Benutzerauthentifizierung und -autorisierung bereitgestellt und kann von verschiedenen Anwendungen über Docker-Container Authentifizierungsmechanismen einrichten.

Monitoring

Im Überwachungsbereich werden alle vorhandenen Dienste mittels Docker-Containern der Cloud-Infrastruktur auditiert und beinhaltet dieser die Open-Source-Software Grafana zur Visualisierung und Überwachung von Leistungsdaten, sowie Uptime Kuma als Webserver für Statusseiten und Healthchecks, um die Verfügbarkeit der Dienste zu kontrollieren.

DevOps

Der Fokus dieses Bereiches liegt bei den Anwendungen in der Entwicklung und Bereitstellung und enthält die Kollaborationsplattform GitLab, um Projekte zu verwalten. Dabei werden diese Dienste mittels Docker-Containern hochgefahren. Nexus kommt als Verwaltungstool der Repositories für die Anwendungsabhängigkeiten zum Einsatz. Sonarqube ermöglicht die statische Analyse und Bewertung der Quelltextqualität. Zusätzlich wird SFTPGO verwendet, um sichere Authentifizierungsmethoden, wie zum Beispiel SSH-Schlüssel und Passwörter zu verwalten.

E-Mail-Kommunikation

In diesem Bereich werden Docker-Container eingesetzt, der den Mail-Server Mailcow hochfährt, um E-Mails zu senden und zu empfangen, SOGO als Groupware-Lösung, was eine effiziente E-Mail-Kommunikation und Zusammenarbeit innerhalb und außerhalb des Unternehmens ermöglicht. Insgesamt werden für dieses Projekt drei Instanzen verwendet. Zum Einen ist es die **"control_node"** als eine Instanz, auf welcher sich zu Beginn die Benutzer/-innen verbinden, woraufhin die folgende Verbindung auf die nächste Instanz, entweder der auf den **"rev_prox_dev"** oder der **"tal_cloud_infra"** über SSH ablaufen. Dabei befinden sich alle Services in den oben genannten Bereichen auf der **"tal_cloud_infra"** außer der NGinx Reverse Proxy Manager, der auf dem **"rev_prox_dev"** lokalisiert ist. Eine Vorschau der Cloud-Infrastruktur befindet sich im Anhang im Kapitel A.5 in der Cloud-Infrastruktur auf der Seite iv. Eine Darstellung, wie der Zugriff eines Users/ Entwicklers auf

1 Einleitung

eine Instanz über die CLI erhält, befindet sich im Anhang A.4 Sequenzdiagramm CLI Zugriff auf die Instanzen.

1.4.2 Organisatorisch

Nach der Implementierung Authentiks in der Cloud-Umgebung, erfolgen erste Tests und Validierungen in den erstellten Docker-Containern via 'docker-compose.yml-Dateien', um sicherzustellen, dass die MFA ordnungsgemäß funktioniert und den Sicherheitsanforderungen entspricht. Im Anschluss erfolgen Schulungen der Benutzer, in dem Fall das Entwicklerteam, zur genauen Verwendung von Authentik mit MFA. Nach den Tests und der Schulungen wird die Authentik-MFA-Implementierung in der Cloud-Umgebung bereitgestellt.

1.4.3 Personell

Das Projektteam besteht aus folgenden Personen:

- Projektauftraggeber/ Director: Herr Dr. Volker Stroetmann
- Projektleiter/ Manager/ Projektentwickler: Herr Edgar Johann Kapler
- Projektentwickler/ Auszubildender: Herr Dmytro Datsiuk
- Projektentwickler/ dualer Student: Herr Neo-Pascal Loest
- Projektentwicklerin/ duale Studentin: Frau Martyna Mol
- Projektentwickler/ Auszubildender: Herr Angelo Juliano Vogt
- Projektentwicklerin/ Auszubildende: Frau Melissa Futtig

Der Projektauftraggeber und -leiter sind die Verantwortlichen für die Projektleitung und -finanzierung des Projektes. Sie genehmigen dieses und stellen die notwendigen Ressourcen zur Entwicklung bereit. Die Projektentwickler: innen sind die allgemeinen Benutzer und das Entwicklerteam. Sie sind für die Umsetzung und den reibungslosen Betrieb der Cloud-Infrastruktur verantwortlich und benötigen sichere Zugriffsmöglichkeiten zu den bereitgestellten Anwendungen.

2 Projektplanung

2 Projektplanung**2.1 Projektphasen**

Die im Projektantrag festgelegten Projektphasen lassen sich chronologisch in die 5-stündige Planungsphase, die 16-stündige Implementierungsphase, die 6-stündige Testphase, die 4-stündige Phase einteilen, in der die Einführung und Übergabe erfolgt und die 7-stündige Dokumentation im Anschluss. Dabei änderte sich die Zeit in der Implementierungsphase von 14 auf 16 Stunden, die Zeit in der Dokumentation von 6 auf 7 Stunden.

Das Projekt findet in zwei Wochen, vom 30.10.2023 bis zum 10.11.2023 statt. Grund dafür ist ein Feiertag und ein möglicher entstehender Krankheitsfall.

Tabelle 1 zeigt ein Beispiel für eine grobe Zeitplanung.

Projektphase	Geplante Zeit
Planungsphase	8 h
Implementierungsphase	16 h
Testphase	4 h
Einführung und Übergabe	4 h
Dokumentation	8 h
Gesamt	40 h

Tabelle 1: Zeitplanung

Eine detailliertere Zeitplanung findet sich im Anhang A.2: Detaillierte Zeitplanung auf Seite ii.

2.2 Abweichungen vom Projektantrag

Die im Projektantrag mit in *Auflage genehmigten* Inhalten, erforderten Änderungen in der Projektdokumentation. Einige Änderungen sind im Kapitel 4 Authentifizierungs-Tool einsehbar. Änderungen:

- gesamte Zeitplanung - von 35 auf 40 Stunden gestreckt
- Stundenplanung - Planungsphase von 5 auf 8 Stunden
- Stundenplanung - Implementierungsphase von 14 auf 16 Stunden
- Stundenplanung - Tesphase von 6 auf 4 Stunden
- Stundenplanung - Dokumentation von 8 auf 6 Stunden
- Zeitplanung/ Planungsphase - *Klärung der Projektziele* nach *vorn* der Phase geschoben
- Zeitplanung/ Dokumentation - *Benutzerdokumentation* statt Entwicklerdokumentation
- Implementierungsphase/ Installation und Konfiguration von Sitecars - *Authentik* statt Sitecars

2 Projektplanung

2.3 Ressourcenplanung

2.3.1 Sachmittelplanung

Um die Umsetzung des Projektes zu ermöglichen, wurden folgende Hard- und Software verwendet:

- Notebook - Lenovo ThinkPad T15 Gen 1 (für die Entwicklung)
- Betriebssystem - Microsoft Windows 10 Enterprise auf dem Lenovo-Notebook
- iPhone 12 - iOS 17.0.3 (zum Testen des Einmalpassworts)
- Microsoft Authenticator (auf dem iPhone 12 vorinstalliert)
- IDE - Visual Studio Code 1.83.1 (user setup)
- Docker-Containerisierung auf der OVHCloud-Infrastruktur in einer Linux-Umgebung
- OVHCloud-Instanz - firewall_instance_dev (flavor name: b2-7)
- OVHCloud-Instanz - tal_cloud_infra (flavor name: r2-60)
- OVHCloud-Instanz - rev_prox-dev (flavor name: b2-15)

2.3.2 Personalplanung

Tabelle 2 zeigt die Personalplanung des Projektes.

Name	Rolle/ Berufsbezeichnung	Zeitaufwand
Dr. Volker Stroetmann	Director	0 h
Edgar Johann Kapler	Manager	1 h
Neo-Pascal Loest	dualer Student	0 h
Martyna Mol	duale Studentin	0 h
Birk Spinn	dualer Student	4 h
Dmytro Datsiuk	Auszubildender	0 h
Angelo Juliano Vogt	Auszubildender	0 h
Melissa Futtig	Auszubildende	42 h

Tabelle 2: Personalplanung

2 Projektplanung

2.3.3 Ablaufplanung und Meilensteine

Die Ablaufplanung ist mit einem Gantt-Diagramm und Meilensteine im Kapitel A.1 des Anhangs dargestellt. Dabei stellt die Farbe pink *keine Arbeitszeit* an dem Tag dar, die Farbe grün eine *reine Arbeitszeit* von 8 Stunden am Tag und die hellblaue Farbe einen *halben Arbeitstag* von 4 Stunden. Die jeweiligen Phasen werden mit Meilensteinen abgeschlossen. Die erste Phase startet am Mittwoch, den 01.11.2023, während die letzte mit ihrem Meilenstein am 08.11.2023 endet. Dabei erfolgt die reguläre Arbeitszeit in einer normalen Arbeitswoche von Montag bis Freitag.

2.4 Entwicklungsprozess

Das Projekt unterteilt sich in einem überschaubaren, zeitlich und inhaltlich begrenzten Entwicklungsprozess mit gesondert begrenzten Phasen, die nach- und voneinander aufbauen. So wird eine Sicherstellung der Schritt- für Schritt-Fertigstellung der jeweiligen Phasen und Übersicht garantiert. Bedingt dessen, dass das Projekt klare Anforderungen hat, welche umfassend mit vorhersehbaren Bedingungen formuliert sind und einen linearen Fortschritt ermöglicht, braucht die agile Methode nicht verwendet zu werden. Auch ist der Umfang des Projektes zeitlich abgegrenzt und besitzt eine strukturierte Vorgehensweise mit einer geringen Interaktion mit dem Entwicklerteam und dem Projektleiter als Kunden.

2.5 Anforderungsanalyse

2.5.1 Funktional

Authenik muss folgende funktionale Anforderungen erfüllen:

- problemlose Registrierung und einfacher Login
- nachvollziehbare Schritte während der Anmeldung bei der Eingabe des Einmalpassworts
- übersichtliche Darstellung und Verwaltung der einzuloggenden Nutzer :innen
- Login als Admin und durchschnittlicher User
- vor jeden konfigurierten Service schalten und nach Eingabe der Nutzerdaten freigeben
- muss sicher sein und Zugriff von Dritten verweigern
- kompatibel mit einer Authenticator-Software
- schnelle Eingabe der Nutzerdaten

3 Analysephase

2.5.2 Nicht-Funktional

Authentik muss folgende nicht-funktionale Anforderungen erfüllen:

- Skalierbarkeit der Services
- das Überleiten auf den nächsten Service sollte in weniger als 2 Sekunden geladen haben
- Enthalten des Brandings von der Deloitte Wirtschaftsprüfungsgesellschaft GmbH
- übersichtliche, englischsprachiges Willkommens-Display

3 Analysephase

3.1 Ist-Analyse

Das Projekt, operiert durch die Deloitte Wirtschaftsprüfungsgesellschaft GmbH, verwendet die Cloud-Infrastruktur von OVHCloud, um einen Business Hosting Service bereitzustellen. Dabei enthält die Konfiguration der Cloud-Umgebung eine Firewall, welche eine öffentliche IP-Adresse zugewiesen wurde. Zusätzlich sollte erwähnt werden, dass dieses Netzwerk privat ist und andere Services und Instanzen enthält, welche von der Firewall geschützt werden. Um einen Zugriff auf die Instanzen zu ermöglichen, wird den Command-Line-Interface-Nutzer/-innen mit einem gültigen SSH-Schlüssel die Möglichkeit geboten, über die Kontrollinstanz *control_node* auf die anderen Instanzen zuzugreifen. Die anderen für das Projekt relevanten Instanzen sind *rev_proxy_dev* und *tal_cloud_infra* auf denen sich, die im Kapitel 1.4.1 Technische Projektschnittstellen erwähnten Instanzen befinden. Die Graphical-User-Interface-Nutzer/-innen können die Services über den NGinx Reverse Proxy Manager zu erreichen, indem der Zugriff klassisch mittels einer einfachen Nutzer- und Passworteingabe, ohne einer weiteren Schutzebene erfolgt.

3.2 Soll-Analyse

Das Soll des Projektes ist es die Dienste mittels Authentik durch die MFA zu schützen. Dabei wird vor jedem Service der Identity-Provider Authentik vorgeschalten, sodass nicht nur MFA, sondern auch SSO passiert und die Benutzer/-innen automatisch authentifiziert werden und das Schutzziel Authentizität erfüllt wird.

Schlussfolgernd ist zu sagen, dass die Benutzer/-innen sich vor jeder Anmeldung bei einem Service erst bei Authentik anmelden, um auf den gewünschten Dienst zugreifen zu können.

3 Analysephase

3.3 Wirtschaftlichkeitsanalyse

Durch die schon vorhandene Cloud-Infrastruktur entstehen keine weiteren Kosten. Bedingt dessen, dass die OVH-Cloud-Infrastruktur zu einem Fix-Preis pro Instanz gemietet wird und keine weiteren Instanzen für die Implementierung des Tochter-Projektes erforderlich sind. An Ressourcen wird Speicher und mehr Rechenleistung benötigt, welche auf der vorhandenen Instanz zur Verfügung stehen und die beiden Faktoren das Arbeiten der Instanz nicht beeinträchtigen und resultierend daraus keine größere Instanz notwendig ist. Die wirklich zu entstehenden Kosten sind ausschließlich Personal- und Materialkosten, wobei letztere aus der Nutzung des Büromöbelars zusammengefasst wird.

Durch die Einführung von MFA durch Authentik in der Cloud-Infrastruktur werden besonders die Schutzziele der Einhaltung der Integrität und Vertraulichkeit der Daten auf den jeweiligen Diensten eingehalten. So wird die Sicherheit erheblich verbessert und trägt dazu bei, unbefugten Zugriff, Datenverluste und Betrug zu verhindern. Dieser Schutz vor Sicherheitsverletzungen kann signifikante finanzielle Auswirkungen haben, da die Wiederherstellungskosten vermieden werden können. Des Weiteren erfolgen Kostenersparnisse in dem Punkt des Verhinderns der Passwort-Resets durch das Anfragen des administrativen Supports, bei welchem Zeit und daraus Kosten entstehen, die vermieden werden können. Durch die Implementierung kann den Nutzer/-innen ein sicherer und bequemer Zugriff gewährleistet und die Kosten gesenkt werden.

3.3.1 „Make or Buy“-Entscheidung

In der Entscheidungsmatrix für die Zielplattform aus dem Kapitel 4.2: Authentifizierungs-Tool auf der Seite 10 sind einige alternative Produkte sichtbar, welche wie Authentik, implementiert werden müssen.

3.3.2 Projektkosten

Die Kosten für die Durchführung des Projekts setzen sich aus den Personal- und Ressourcenkosten zusammen.

$$8 \text{ h/Tag} \cdot 220 \text{ Tage/Jahr} = 1760 \text{ h/Jahr} \quad (1)$$

$$1400 \text{ €/Monat} \cdot 12 \text{ Monate/Jahr} = 16800 \text{ €/Jahr} \quad (2)$$

$$\frac{16800 \text{ €/Jahr}}{1760 \text{ h/Jahr}} \approx 9,55 \text{ €/h} \quad (3)$$

Anhand der oben genannten Formel ergibt sich ein Stundenlohn von 9,55 €.

Die Durchführungszeit des Projekts beträgt 40 Stunden. Dabei sind mögliche Ressourcen, wie der Stromverbrauch, die zu verwendende Hardware und die Räumlichkeiten, sowie das Büromaterial, wie

3 Analysephase

z. B. der zu nutzende Monitor, die Peripheriegeräte (Maus, Tastatur, etc.) oder das Möbelar, was pauschal mit 15,00 € kalkuliert werden kann. Das Brutto-Einkommen eines Auszubildenden im 3. Lehrjahr im Fachbereich Fachinformatik bei der Deloitte Wirtschaftsprüfungsgesellschaft GmbH beträgt 1400,00 € pro Monat. Für die weiteren Mitarbeiter/-innen werden pauschale Beträge zur Berechnung des Stundensatzes genutzt, aus den Gründen, dass die Deloitte Wirtschaftsprüfungsgesellschaft GmbH die Kosten pro Stunde nicht preisgeben möchte. Duale Student/-innen werden pauschal mit 15,00 €, während der Manager mit 50,00 € pro Stunde berechnet werden. Bei jeweils beiden addiert sich die Summe der Ressourcenkosten auf. Die Gesamtkosten, dargestellt in der Tabelle 3, betragen 1228,78 €.

Vorgang	Zeit	Kosten pro Stunde	Kosten
Arbeitskosten	41 h	9,55 € + 15,00 € = 24,55 €	1031,10 €
Unterstützungskosten (Manager)	1 h	50,00 € + 15,00 € = 65,00 €	65,00 €
Unterstützungskosten (dualer Student)	4 h	15,00 € + 15,00 € = 30,00 €	120,00 €
Abnahmetest	1 h	25,00 € + 15,00 € = 40,00 €	80 €
OVHCloud-Kosten	40 h	0,317 € + 0,00 € = 0,317 €	12,68 €
			1.228,78 €

Tabelle 3: Kostenaufstellung

3.3.3 Amortisationsdauer

Die Amortisation beschleunigt sich durch die Verwendung von Docker, GitLab und Authentik, was die Einsparung von Lizenzkosten zur Folge hat. Grund dafür ist, dass diese Plattformen Open-Source sind und kostenlos genutzt werden können, was zu einer Reduzierung der Gesamtbetriebskosten (Total Cost of Ownerships (TCO)) führt. Im Vergleich zu einigen kostenpflichtigen Virtualisierungslösungen, wie z. B. Microsoft Hyper-V, können also Lizenzkosten eingespart werden. Des Weiteren ermöglicht Docker eine Arbeitszeitzersparnis durch die einfache Bereitstellung und Verwaltung von Diensten, was die Arbeitszeit für die Einrichtung und Wartung von Umgebungen verkürzt.

3.4 Nicht-monetärer Nutzen

Für das Projekt werden die Produkte Authelia, Authentik, Microsoft Azure AD und Sitecar, zur Implementierung in Erwägung gezogen. Wobei mittels einer Nutzwertanalyse, welche im Kapitel ??: ?? zu sehen ist, der Sachverhalt durch eine Entscheidungsmatrix dargestellt wird.

Da die Ergebnisse der Wirtschaftlichkeitsanalyse bereits eine ausreichende Begründung für die Umsetzung des Projekts bieten, ist es an dieser Stelle nicht notwendig, eine eingehende Untersuchung der nicht-monetären Vorteile vorzunehmen.

Ohne der Einführung eines Authentifizierungs-Tools wird die Sicherheit der angebotenen Dienste nicht geboten und das Risiko des Datenverlustes gewährleistet. Um das Risiko zu minimieren, soll durch die

4 Entwurfsphase

Nutzwertanalyse ein Ergebnis und die Entscheidungsfindung der jeweiligen Authentifizierungsmethode erleichtert werden.

3.5 Anwendungsfälle

Ein Use Case-Diagramm zur Veranschaulichung des Prozesses der Cloud-Infrastruktur findet sich im Anhang A.3: Use Case-Diagramm auf Seite iii. In diesem interagiert der Akteur aus der Sicht eines Projektentwicklers mit dem System, in welchem verschiedene Anwendungsfälle existieren. Der Akteur meldet sich über den Authentik Server bei der Firewall und dem NGinx Reverse Proxy Manager an. Nach der erfolgreicher Anmeldung mit der MFA hat dieser die Möglichkeit auf die dann zur Verfügung stehenden Dienste vom Nginx Reverse Proxy Manager aus zuzugreifen.

Hat sich der Akteur mit dem Authentik Server verbunden, der aus dem eigentlichen Server (Authentik Server Core) und dem integrierten Außenposten (Embedded outpost) besteht. Einkommende Anfragen an den Server-Containern werden an den Authentik Server Core or dem Embedded outpost geroutet. Der Authentik Core Server verarbeitet den Großteil der Logik von Authentik, wie z. B. API- und/oder SSO-Anfragen, während der Embedded outpost die Verwendung von Proxy-Anbietern ermöglicht, ohne dass eine separate Außenstelle eingerichtet werden muss. Der Hintergrundarbeiter (Background Worker) führt Hintergrundaufgaben aus, wie das Senden von E-Mails, oder Benachrichtigungen von Ereignissen und alles, was im Frontend sichtbar ist. Authentik nutzt PostgreSQL, um alle seiner Konfigurationen und Daten zu speichern. Redis wird als Message-Queue und Cache verwendet.

4 Entwurfsphase

4.1 Zielplattform

Die zu resultierende Zielplattform definiert sich über die Benutzerfreundlichkeit, die Sicherheit und dem Fokus auf der Interaktion mit OIDC und LDAP, welcher zukünftig für das Projekt vorgesehen sind, sowie der Implementierung vom Open-Source, dem Arbeiten mit MFA, der Skalierbarkeit und den Erfahrungswerten von anderen Entwicklern mit dem entsprechenden Produkt. Das Resultat wird im Kapitel 4.2: Authentifizierungs-Tool der dargestellten Entscheidungsmatrix sichtbar.

4.2 Authentifizierungs-Tool

Anhand der Entscheidungsmatrix in Tabelle 4 wurde Authentik ausgewählt.

Die in Kapitel 4.1: Zielplattform erwähnten Eigenschaften tragen zur Entscheidungsfindung bei, sodass sich anhand der gegebenen Entscheidungsmatrix Authentik herauskristallisierte.

Die Gewichtung hat einen Gesamtwert von 100 Wertungspunkten mit einem Maximalwert von 25

4 Entwurfsphase

Eigenschaft	Wertung	Authentik	Authelia	Sitecar	Micr. Az. AD
Benutzerfreundlichkeit	15	15	15	12	14
Sicherheit (OIDC, LDAP)	25	25	17	18	20
Open-Source	15	15	15	9	7
MFA	20	19	20	14	19
Skalierbarkeit	15	12	14	12	15
Erfahrungswerte	10	7	9	3	10
Gesamt:	100	93	90	68	85
Nutzwert:		17,05	15,75	12,55	15,20

Tabelle 4: Entscheidungsmatrix

und Mindestwert von 10. Grund dafür sind die unterschiedlichen Eigenschaften, welche in der Entwicklung und bei der Auswahl der Authentifizierungsmethode jeweils verschiedene Rollen spielen und folglich daraus evaluiert werden. Nach der Zuordnung und Addierung der Punkte bei den vier Authentifizierungs-Tools, wird die Gesamtheit aller Punkt eines Produktes durch den Wert 100 dividiert und das Endergebnis ausgerechnet. Dabei hat die Einhaltung der Sicherheit Priorität und erhält den Maximalwert von 25 Punkten, aufgrund dessen, dass Dritten der Zugriff auf die jeweiligen Dienste mit kunden- und firmeninternen Daten der Cloud-Infrastruktur verweigert werden sollte. Die MFA wird mit 20 Punkten bewertet, weil das das Ziel des Projektes ist. Die Benutzerfreundlichkeit, das Implementieren mit Open-Source und die Skalierbarkeit erhalten 15 Punkte, weil jeder User schnell und einfach auf den jeweiligen Dienst zugreifen muss. Für dieses Projekt ist es des Weiteren wichtig, ein Tool zu implementieren, was den zeitlichen Rahmen nicht überschreitet und die Gesamtheit der Einführung zu komplex gestaltet. Die Skalierbarkeit hat für das Projekt eine durchschnittliche Relevanz, da die Möglichkeit besteht, Dienste hinzuzufügen oder rauszunehmen. Am wenigsten bedeutend sind die Erfahrungswerte, welche gleichermaßen nicht zu unterschätzen ist, da eine Community über das Produkt bei der Entwicklung unterstützend wirkend kann.

Den größten Nutzwert erhält Authentik mit 17,05 Punkten und schneidet vor Authelia, Microsoft Azure AD und Sitecar am besten ab. Aus diesem Grund wird sich für Authentik anstatt für Sitecar entschieden, da besonders die Implementierungsdauer und -komplexität bei Sitecar den Rahmen des Projektes sprechen würde.

4.3 Geschäftslogik

Im Anhang befindet sich eine genaue Darstellung der Cloud-Infrastruktur und des Use Case-Diagramms, sowie das ?? zur besseren Visualisierung.

Die Implementierung von Authentik erleichtert den Entwicklern den Arbeitsfluss durch das einmalige Anmelden bei allen Diensten.

5 Projektdurchführung

4.4 Maßnahmen zur Qualitätssicherung

4.4.1 Produktorientierte Maßnahmen

4.4.2 Prozessorientierte Maßnahmen

Durch die kontinuierliche Anwendung des Qualitätsmanagementsystems gemäß ISO 9001 im Qualitätsmanagement erfolgt nach der Planung eine sorgfältige Überprüfung jedes Schrittes auf Richtigkeit. Bei festgestellten Fehlern wird nach alternativen Wegen zur Zielerreichung gesucht, um schließlich erfolgreich umzusetzen. Dieser Prozess folgt dem Plan-Do-Check-Act-Zyklus.

Als Online-Dienstleister ist es laut den Vorschriften des Bundesamts für Sicherheit in der Informatstechnik (BSI) zwingend erforderlich, Daten und Geräte durch eine Mehrfaktor-Authentifizierung (MFA) zu schützen, bei der der Login durch die Verwendung eines Passworts und eines weiteren Faktors abgesichert wird. Authentik, als Identitätsprovider, nutzt ein Informationssicherheitssystem, das auf etablierten Standards wie BSI100-2 und ISO27001 basiert.

5 Projektdurchführung

5.1 Vorbereitung der Entwicklungsumgebung

Die Voraussetzung zur Implementierung von Authentik ist, dass Docker und Docker Compose auf dem im Kapitel 2.3.1 Sachmittelplanung erwähnten Notebook vorinstalliert sind und einen Zugang zum Internet verfügen. Des Weiteren sollten die zu benötigenden Hard- und Softwarekomponenten, welche ebenfalls in der Sachmittelplanung auf der Seite 5 gelistet sind, funktionierend sein. Wichtig für die Durchführung ist nicht nur Docker mit dem Notebook selbst, sondern auch der Besitz einer Domain oder Subdomain, welche bei der Deloitte Wirtschaftsprüfungsgesellschaft GmbH, die tal.deloitte.de ist. Diese muss entweder mit einem A- oder CNAME-Record versehen sein. Um die Domain-Namen übersichtlich verwalten zu können, empfiehlt sich ein Reverse Proxy, in diesem Fall wird es auf den NGinx Proxy Manager zurückzuführen sein. Und zu guter Letzt einen SMTP E-Mail Server zur beispielweise Zurücksetzung eines Passworts. Für das Testen der kommenden Schritte im Kapitel 5.7 Konfiguration des zweiten Faktors ab der Seite 15 wird das iPhone 12, erwähnt in der Sachmittelplanung, verwendet. Dieses mobile Endgerät ist ein Firmentelefon und beinhaltet zusätzlich den Microsoft Authenticator, um sich gewissermaßen remote mit dem VPN des Firmennetzwerkes verbinden zu können. Aus diesem Grund muss kein weiteres Active Directory installiert und eingerichtet werden.

5.2 Auswahl einer MFA-Lösung

Bei Authentik werden die drei Optionen **WebAuthn Authenticator Setup Stage**, **Static Authenticator Stage** und **TOTP Authenticator Setup Stage** angeboten.

Das Ergebnis der Tabelle 5 Nutzwertanalyse zur MFA-Lösung ist nicht eindeutig zuordbar, bedingt

5 Projektdurchführung

dessen, dass die Optionen WebAuthn Authenticator Setup Stage und TOTP Authenticator Setup Stage um 0,05 Wertungspunkte auseinander liegen und die Entscheidung des finalen Ergebnisses nicht anhand der Nutzwertanalyse zur MFA-Lösung manifestierend festzulegen ist.

Eigenschaft	Wertung	WebAuthn	Static	TOTP
Implementierungsaufwand (niedrig)	25	12	25	18
Zeitersparnis Eingabe	20	14	16	15
Sicherheit	35	35	25	30
Benutzerakzeptanz	20	18	15	18
Gesamt:	100	79	81	81
Nutzwert:		21,65	21,2	21,6

Tabelle 5: Nutzwertanalyse zur MFA-Lösung

Die Entscheidungstreffung erfolgte besonders auf der Prämisse, dass die Deloitte Wirtschaftsprüfungs-gesellschaft GmbH das TOTP-Verfahren, quasi die Eingabe eines Einmalpassworts durch einen Authenticator, wie das iPhone 12, gestellt durch die Deloitte, bei allen zur Verfügung stehenden Services verwendet. So fiel die Entscheidung auf das **TOTP-Verfahren**, was hingegen zum WebAuth Authenticator Setup Stage weniger Sicherheit aber weniger Implementierungsaufwand erfordert und kein weiteres Gerät oder eine weitere Datei oder Software notwendig ist, um die in der zu entstehenden hardwarebasierten Token zu verwalten. In dem TOTP Authenticator Setup Stage geben die Entwickler :innen alle zu Beginn ihren Nutzernamen und das zugehörige Passwort ein. Nach einer erfolgreichen Anmeldung, werden die Entwickler :innen weitergeleitet, um ihren 6-stelligen Zahlencode, der in dem Microsoft Authenticator für 30 Sekunden sichtbar ist, einzugeben. Wenn die Entwickler :innen sich noch nicht über Authentik angemeldet hatten, werden diese nach der Anmeldung mit einem QR-Code gepromptet und daraufhin aufgefordert den 6-stelligen Code einzugeben.

5.3 Erstellung der docker-compose.yml, .env

Um Authentik über eine "docker-compose.yml"-Datei im Anhang des Kapitels A.6 zum Laufen zu bringen, ist es erforderlich, dass nicht nur der Authentik-Server, sondern auch der Authentik-Worker, Redis und PostgreSQL gleichzeitig erstellt werden. PostgreSQL ist eine objektrelationale Datenbank und unterstützt die Erweiter- und Skalierbarkeit der Cloud-Infrastruktur. Redis hingegen ist ein In-Memory-Datenspeicher, der als schneller Datenspeicher dient. Die ".env"-Datei im Kapitel A.7 .env enthält die individuellen Umgebungsvariablen für die Zugangsdaten der Nutzer :innen.

Beide Dateien werden in einem Ordner "Authentik" auf der Instanz "**tal_cloud_infra**" durch docker erstellt. Eine Darstellung der Instanzen befindet sich im Kapitel A.5 Cloud-Infrastruktur auf der Seite iv. Die "docker-compose.yml"-Datei wurde über [Composerize](#), einer Applikation aus dem Internet entnommen, welche öffentlich zugänglich ist. Auch die ".env"-Datei ist öffentlich über die Webpage von [Authentik](#) einsehbar. Die einzigen in dieser Datei vorzunehmenden Änderungen, sind die Variablen: "PG_PASS", "AUTHENTIK_SECRET_KEY", "AUTHENTIK_EMAIL_HOST", "AUTHENTIK_EMAIL_USERNAME", sowie "AUTHENTIK_EMAIL_PASSWORD" und "AUTHEN-

5 Projektdurchführung

TIK_EMAIL__FROM". Um Authentik zu starten, werden beide Dateien im Unterordner Authentik eingefügt. Nun wird mit dem Befehl **docker-compose pull** in Docker Compose die **docker-compose.yml** mit deren enthaltenen Diensten heruntergeladen, die Images und Volumes heruntergezogen. Mit dem Befehl **docker-compose up -d** erfolgt zu Beginn die Sicherstellung, dass das docker-compose.yml wirklich vorhanden ist, um dann gelesen und den Container für die darin definierten Dienste im Hintergrund zu starten. Der Parameter **-d** (**--detach**) bewirkt, dass die Container im Hintergrund ausgeführt werden. Nach dem Start der Container erfolgt die Statusüberprüfung dieser mit dem Befehl **docker-compose ps**.

5.4 Konfiguration des NGinx Reverse Proxy Managers

Nachdem Authentik in einem Docker-Container läuft, erfolgt die Konfiguration des NGinx Reverse Proxy Managers:

1. Erstellung einer Authentifizierungs-Domain (auth.example.domain) und Einstellung eines A-Records im DNS-Resolver
2. Im NGinx Reverse Proxy Managers einen neuen Host erstellen, was im Anhang in der Proxy Host Konfiguration einsehbar ist
3. private IP-Adresse des Authentik-Servers mit der in der **.env**-Datei eingegebenen Portnummer (80) eingeben mit dem Resultat für das Beispiel: **0.0.0.0:80** - Einsicht im A.8 Proxy Host Konfiguration
4. im SSL-Tab des Konfigurationsfeldes, anklicken: *Force SSL, HTTP/2 Support, HSTS Enabled* und *HSTS Subdomains*
5. im E-Mail Feld die E-Mail Adresse (admin@example.domain.de) eingeben und den Nutzungsbedingungen zustimmen
6. Ergebnis: Zugriff auf Authentik möglich, sodass die Willkommens-Seite sichtbar wird, welche im Anhang im Kapitel A.8 Proxy Host Konfiguration

5.5 Konfiguration von Authentik

Nach der Konfiguration des NGinx Reverse Proxy Managers, werden in Authentik ein Projekt und die vorhandenen User erstellt. Diese Vorgehensweise ist im Anhang in der Authentik Konfiguration detailliert beschrieben.

6 Testphase

5.6 Integration mit Cloud-Diensten

Damit sich Authentik vor jeden Dienst in der gegebenen Cloud-Infrastruktur schalten kann, wird in der Host-Konfiguration im NGinx Reverse Proxy Manager im Bereich *Advanced* die im Anhang erwähnte NGinx Konfiguration einzufügen. Wobei zu beachten ist, dass bei jedem Service die Portnummer geändert wird, sodass eine Umleitung von Authentik auf diesen erfolgen kann.

5.7 Konfiguration des zweiten Faktors

Nach dem Ergebnis aus der Nutzwertanalyse zur MFA-Lösung im Kapitel 5.2 Auswahl einer MFA-Lösung geht das TOTP-Verfahren hervor. Eine mit Bildern behaftete Ansicht befindet sich im Anhang im A.11 TOTP-Konfiguration.

Ein kurze Schrittfolge zur Einrichtung dieses:

1. Login bei Authentik
2. auf **Einstellungen - MFA Devices** bestätigen
3. **Enroll** bestätigen - eine Methode auswählen:
 - WebAuth Authenticator Setup Stage
 - Static Authenticator Stage
 - *TOTP Authenticator Setup Stage* - auswählen
4. Logout bei Authentik
5. erneut Login - QR-Code mit Microsoft AD scannen
6. 6-stelligen Code eingeben und eingeloggt

6 Testphase

6.1 Überwachung der Laufzeit der Services

Die Überwachung der Laufzeit der eingetragenen Dienste passiert über das Dashboard von Authentik. Um jeden einzelnen Dienst schlussendlich zu überprüfen, erfolgte über den NGinx Reverse Proxy Manager ein jeweiliger Zugriff auf alle Dienste, um zu testen, ob sich Authentik auch wirklich vor den Dienst schaltet.

6.2 Überprüfung/ Beseitigung von Fehlern

Nach der erfolgreichen Durchführung des Projektes wurden die Funktionalen und Nicht-Funktionalen Anforderungen aus der Anforderungsanalyse getestet. Das Beseitigen von Fehlern in der Entwicklungsumgebung erfolgte während der Durchführungsphase mittels des Plan-Do-Check-Act-Zyklus, in welchem die Fehlern, z. B. Tippfehler gleich während der Implementierung behoben wurden.

6.3 Zugriffstests

Um den Zugriff zu testen, wurden End-to-End-Tests durchgeführt, die Authentik auf die Gesamtheit überprüfen und sicherstellen, dass die Benutzeranmeldungen und Authentifizierungen erfolgreich verlaufen.

7 Dokumentation

7.1 Benutzerdokumentation

Die Benutzerdokumentation befindet sich im Anhang A.12 Benutzerdokumentation. Darin befindet sich eine kurze Schilderung über den Login bei Authentik mit TOTP.

8 Fazit

8.1 Soll-/Ist-Vergleich

Das Projektziel wurde erfolgreich innerhalb des vorgegebenen Zeitrahmens erreicht. Während der Planung stellte sich jedoch heraus, dass die geschätzte Dauer der Testphase von ursprünglich 6 Stunden zu grob war und stattdessen in 2 Arbeitsstunden abgeschlossen wurde. Daher wurden die übrigen 4 Stunden zur Verbesserung der Dokumentation verwendet. Diese Veränderung von 6 auf 2 Stunden in der Projektumsetzung und Dokumentation erfolgte. Die geplanten Arbeitsstunden für die beiden beteiligten Teammitglieder wurden voll ausgeschöpft, und die Ressourcen, wie in der Sachmittelplanung beschrieben, wurden effizient genutzt.

Wie in Tabelle 6 Soll-/Ist-Vergleich zu erkennen ist, konnte die Zeitplanung bis auf wenige Ausnahmen eingehalten werden.

8 Fazit

Phase	Geplant	Tatsächlich	Differenz
Planungsphase	8 h	8 h	h
Implementierungsphase	16 h	16 h	
Testphase	4 h	3 h	-1 h
Einführung und Übergabe	4 h	4 h	
Dokumentation	8 h	9 h	+1 h
Gesamt	40 h	40 h	

Tabelle 6: Soll-/Ist-Vergleich

8.2 Lessons Learned

Die Zeitplaung und Schätzung der Testphase erwies sich als zu grob und ungenau. Es ist wichtig zu beachten, realistische Zeitpläne zu erstellen und eventuell genügend Puffer einzukalkulieren. Bedingt dessen, dass die Dokumentation ein integraler Bestandteil der Projektarbeit ist, wurde die verkürzte Zeit für die testphase sinnvoll für die Verbesserung der Inhalte in der Dokumentation genutzt. Ein Vorteil der ausgewählten MFA-Lösung ist, dass die Implementierung recht schnell und nachvollziehbar ging.

8.3 Ausblick

Das Projekt ist eine Tochterprojekt eines übergeordneten Projektes. Mit dem Ergebnis wird die Sicherheit der vorhandenen Dienste gewährleistet. Authentik als Identitäts-provider wird weiter ausgebaut, sodass ein Unternehmensdesign zukünftig erstellt wird und Monitoring-Alerts eingefügt, die bei fehlerhaften Logins oder -Logouts eine Mail senden.

Literaturverzeichnis

Literaturverzeichnis

Eidesstattliche Erklärung

Eidesstattliche Erklärung

Ich, Melissa Futtig, versichere hiermit, dass ich meine **Dokumentation zur betrieblichen Projektarbeit** mit dem Thema

Implementierung von MFA – Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe, wobei ich alle wörtlichen und sinngemäßen Zitate als solche gekennzeichnet habe. Die Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt und auch nicht veröffentlicht.

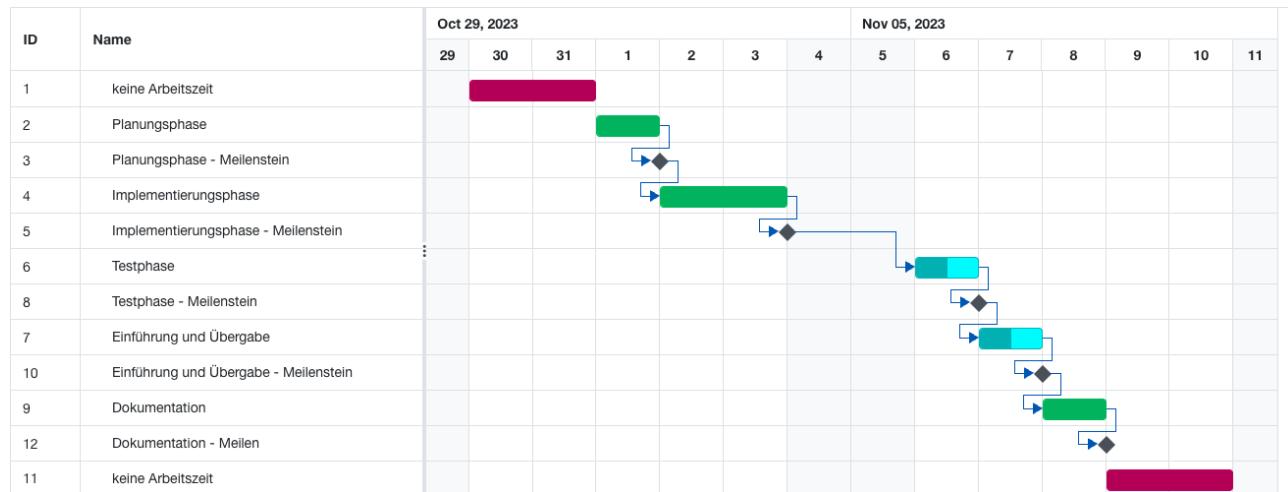
Leipzig, den 10.11.2023

MELISSA FUTTIG

A Anhang

A Anhang

A.1 Gantt-Diagramm und Meilensteine



A.2 Detaillierte Zeitplanung

1. Planungsphase	8 h
1. Klärung der Projektziele	1 h
1.2. Erstellen einer Ist-Analysephase	1.5 h
1.3. Erstellen einer Soll-Analyse	1 h
1.4. Kostenplanung	1.5 h
1.5. Projektumfeldklärung	0.5 h
1.6. Kosten- und Nutzwertanalyse	1.5 h
1.7. Erstellung des Gantt-Diagramms	1 h
2. Implementierungsphase	16 h
2.1. Vorbereitung der Entwicklungsumgebung	1.5 h
2.2 Auswahl einer MFA-Lösung	0.5 h
2.3. Erstellung der docker-compose.yml- und .env-Dateien	2 h
2.4. Installation und Konfiguration von Authentik	5.5 h
2.5. Konfiguration der MFA	2 h
2.6. Integration mit Cloud-Diensten	3.5 h
2.7. Konfiguration des zweiten Faktors	1 h
3. Testphase	4 h
3.1. Überwachung der Laufzeit der Services	0.5 h
3.2. Überprüfung/ Beseitigung von Fehlern	2 h
3.3. Zugriffstest	1.5 h
4. Einführung und Übergabe	4 h
4.1. Ausführung und Ergebnisübergabe	3 h
4.2. Schulung der zu Beteiligten für die Nutzung	1 h
5. Dokumentation	8 h
5.1 Erstellung einer Projektdokumentation der Ergebnisse	7 h
5.3. Erstellung der Benutzerdokumentation	1 h
Gesamt	40 h

A Anhang

A.3 Use Case-Diagramm

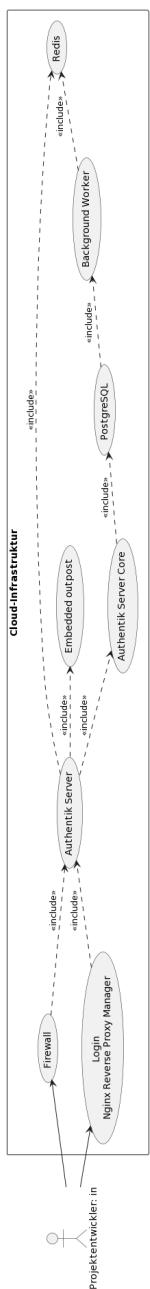
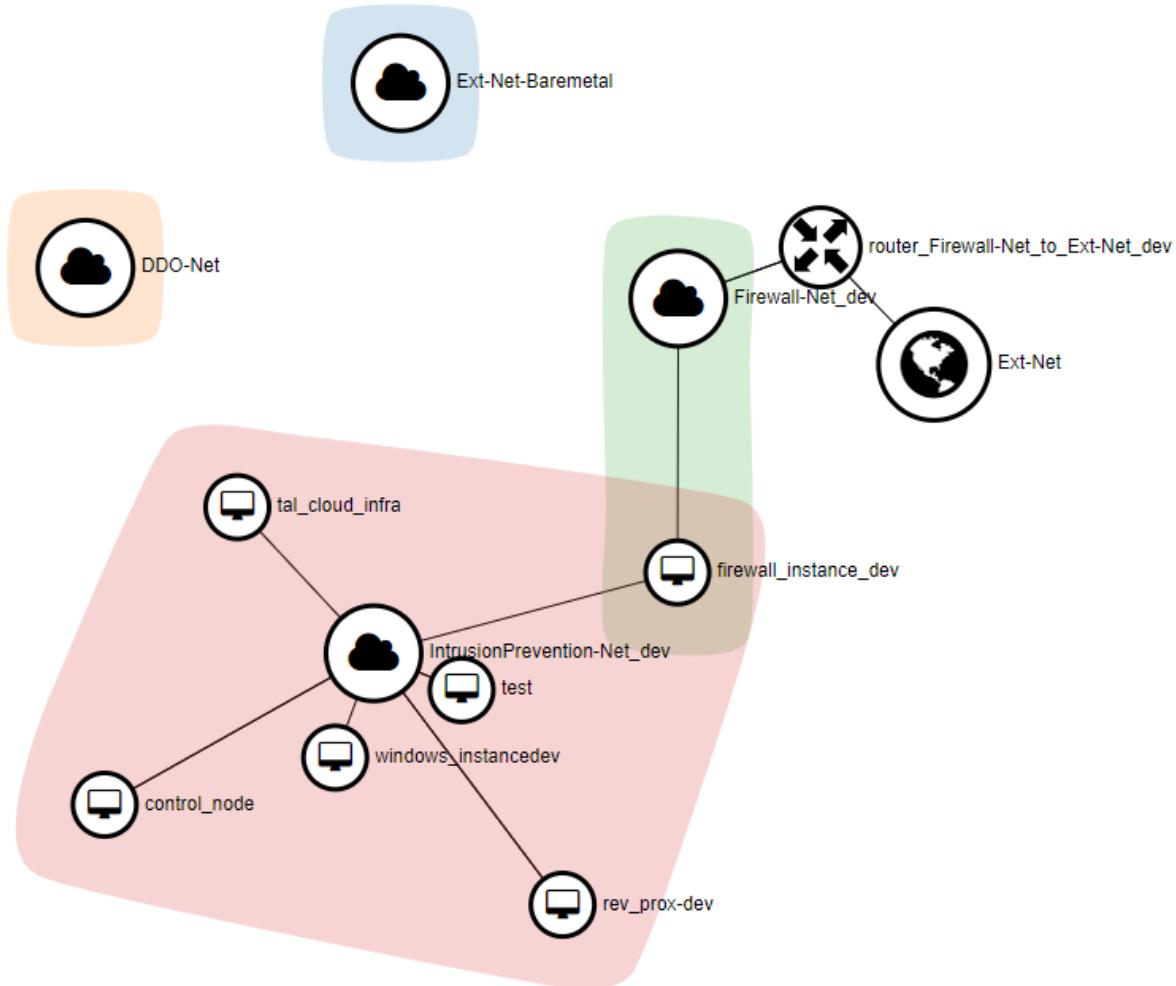


Abbildung 1: Use Case-Diagramm

A Anhang

A.4 Sequenzdiagramm CLI Zugriff auf die Instanzen**A.5 Cloud-Infrastruktur**

A Anhang

A.6 docker-compose.yml

```

version: "3.4"

services:
  postgresql:
    image: docker.io/library/postgres:12-alpine
    restart: unless-stopped
    healthcheck:
      test: ["CMD-SHELL", "pg_isready -d ${POSTGRES_DB} -U ${POSTGRES_USER}" ]
      start_period: 20s
      interval: 30s
      retries: 5
      timeout: 5s
    volumes:
      - ./database:/var/lib/postgresql/data
    environment:
      POSTGRES_PASSWORD: ${PG_PASS:?database password required}
      POSTGRES_USER: ${PG_USER:-authentik}
      POSTGRES_DB: ${PG_DB:-authentik}
    env_file:
      - .env

  redis:
    image: docker.io/library/redis:alpine
    command: --save 60 1 --loglevel warning
    restart: unless-stopped
    healthcheck:
      test: ["CMD-SHELL", "redis-cli ping | grep PONG"]
      start_period: 20s
      interval: 30s
      retries: 5
      timeout: 3s
    volumes:
      - ./redis:/data

  server:
    image: ${AUTHENTIK_IMAGE:-ghcr.io/goauthentik/server}:${AUTHENTIK_TAG:-2023.8.3}
    restart: unless-stopped
    command: server
    environment:
      AUTHENTIK_REDIS_HOST: redis
      AUTHENTIK_POSTGRESQL_HOST: postgresql
      AUTHENTIK_POSTGRESQL_USER: ${PG_USER:-authentik}
      AUTHENTIK_POSTGRESQL_NAME: ${PG_DB:-authentik}
      AUTHENTIK_POSTGRESQL_PASSWORD: ${PG_PASS}
    volumes:
      - ./media:/media
      - ./custom-templates:/templates
    env_file:
      - .env
    ports:
      - "${COMPOSE_PORT_HTTP:-9000}:9000"
      - "${COMPOSE_PORT_HTTPS:-9443}:9443"
    depends_on:
      - postgresql
      - redis

  worker:
    image: ${AUTHENTIK_IMAGE:-ghcr.io/goauthentik/server}:${AUTHENTIK_TAG:-2023.8.3}
    restart: unless-stopped
    command: worker
    environment:
      AUTHENTIK_REDIS_HOST: redis
      AUTHENTIK_POSTGRESQL_HOST: postgresql
      AUTHENTIK_POSTGRESQL_USER: ${PG_USER:-authentik}
      AUTHENTIK_POSTGRESQL_NAME: ${PG_DB:-authentik}
      AUTHENTIK_POSTGRESQL_PASSWORD: ${PG_PASS}
    # `user: root` and the docker socket volume are optional.
    # See more for the docker socket integration here:
    # https://goauthentik.io/docs/outposts/integrations/docker
    # Removing `user: root` also prevents the worker from fixing the permissions
    # on the mounted folders, so when removing this make sure the folders have the correct UID/GID
    # (1000:1000 by default)
    user: root
    volumes:
      - /var/run/docker.sock:/var/run/docker.sock
      - ./media:/media
      - ./certs:/certs
      - ./custom-templates:/templates
    env_file:
      - .env
    depends_on:
      - postgresql
      - redis

volumes:
  database:
    driver: local
  redis:
    driver: local
  
```

PostgreSQL wird installiert
Version 12 wird verwendet
Container startet sich neu, solange er nicht gestoppt wird

Tests des Containers, um sicherzustellen, dass er läuft, wie lange er läuft und ab wann wie oft wiederholt wird

Erstellung eines Speichermediums im Unterordner von Authentik database

Anforderung der Umgebungsvariablen aus der zu erstellten .env-Datei

Redis hilft bei der Zwischenspeicherung
Version alpine wird verwendet
Befehl: Betrieb von Redis soll aufgenommen werden

Erstellung des Speichermediums im Unterordner von Authentik redis

Authentik Server mit dem zu ziehenden Image (Abbildung) der spezifischen Version
Command: Start des Servers
Referenzen zu o.g. Redis und PostgreSQL

Zuordnung der freien Ports für HTTP und HTTPS
abhängig von postgresql und redis

Worker entlastet den Hauptserver

Definition der Volumen (Speichermedien), der inkludierten Datenbank und Reis

A Anhang

A.7 .env

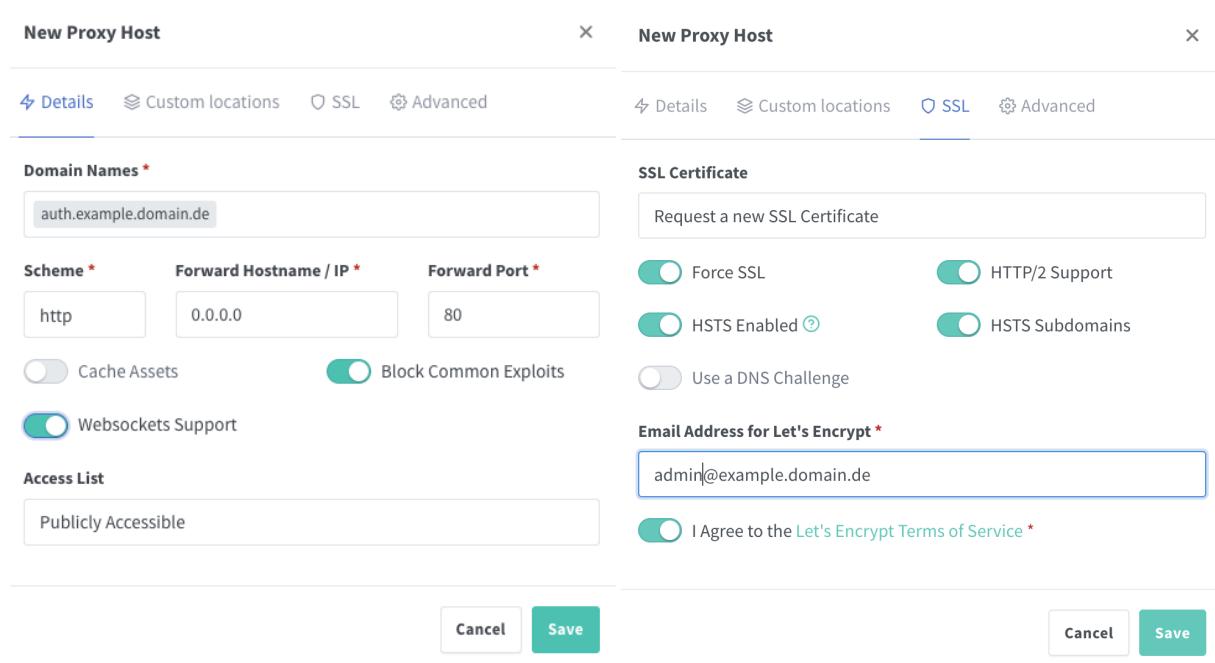
```

PG_USER=authentik
PG_PASS=aReallyLongStrongPasswordShouldBePutHere
sollte ein langes Passwort sein (ab 12 Ziffern)
AUTHENTIK_SECRET_KEY=someincrediblylongcomplexkeygoeshere
sollte eine lange Zeichenfolge von Zahlen, Groß- und Kleinbuchstaben, Symbolen mit mindestens 64 char in der Länge
AUTHENTIK_ERROR_REPORTING_ENABLED=true
# SMTP Host Emails are sent to
AUTHENTIK_EMAIL_HOST=smtp.example.com
Mailadresse mit der Domainname und der Top-Level Domain
AUTHENTIK_EMAIL_PORT=587
# Optionally authenticate (don't add quotation marks to your password)
AUTHENTIK_EMAIL_USERNAME=auth@example.com
Mailadresse mit der Sub- und Top-Level Domain
AUTHENTIK_EMAIL_PASSWORD=a-L0n6-Strong_password_should_go_here
# Use StartTLS
AUTHENTIK_EMAIL_USE_TLS=true
# Use SSL
AUTHENTIK_EMAIL_USE_SSL=false
AUTHENTIK_EMAIL_TIMEOUT=10
# Email address authentik will send from, should have a correct @domain
AUTHENTIK_EMAIL_FROM=auth@example.com
COMPOSE_PORT_HTTP=80
COMPOSE_PORT_HTTPS=443
# Authentik Version to Pull
ATHENTIK_TAG=2023.8.3

```

A Anhang

A.8 Proxy Host Konfiguration



The image displays two side-by-side proxy host configuration forms. The left form is titled "New Proxy Host" and includes sections for "Domain Names" (containing "auth.example.domain.de"), "Scheme" (set to "http"), "Forward Hostname / IP" (set to "0.0.0.0"), "Forward Port" (set to "80"), "Access List" (set to "Publicly Accessible"), and various security and performance options like "Cache Assets" (disabled), "Websockets Support" (enabled), "Block Common Exploits" (enabled), and "SSL" (disabled). The right form is also titled "New Proxy Host" and includes sections for "SSL Certificate" (with a link to "Request a new SSL Certificate"), "SSL" (with options for "Force SSL", "HTTP/2 Support", "HSTS Enabled" (disabled), "HSTS Subdomains" (disabled), and "Use a DNS Challenge" (disabled)), and "Email Address for Let's Encrypt" (containing "admin@example.domain.de") with an "I Agree to the Let's Encrypt Terms of Service" checkbox (disabled). Both forms have "Cancel" and "Save" buttons at the bottom.



A Anhang

A.9 Authentik Konfiguration

A.10 NGinx Konfiguration

```

# Increase buffer size for large headers
# This is needed only if you get 'upstream sent too big header while reading response
# header from upstream' error when trying to access an application protected by goauthentik
proxy_buffers 8 16k;
proxy_buffer_size 32k;

# Make sure not to redirect traffic to a port 4443
port_in_redirect off;

location / {
    # Put your proxy_pass to your application here
    proxy_pass $forward_scheme://$server:$port;
    # Set any other headers your application might need
    # proxy_set_header Host $host;
    # proxy_set_header ...;

    ##### authentik-specific config #####
    auth_request     /outpost.gauthentik.io/auth/nginx;
    error_page        401 = @gauthentik_proxy_signin;
    auth_request_set $auth_cookie $upstream_http_set_cookie;
    add_header        Set-Cookie $auth_cookie;

    # translate headers from the outposts back to the actual upstream
    auth_request_set $authentik_username $upstream_http_x_authentik_username;
    auth_request_set $authentik_groups $upstream_http_x_authentik_groups;
    auth_request_set $authentik_email $upstream_http_x_authentik_email;
    auth_request_set $authentik_name $upstream_http_x_authentik_name;
    auth_request_set $authentik_uid $upstream_http_x_authentik_uid;

    proxy_set_header X-authentik-username $authentik_username;
    proxy_set_header X-authentik-groups $authentik_groups;
    proxy_set_header X-authentik-email $authentik_email;
    proxy_set_header X-authentik-name $authentik_name;
    proxy_set_header X-authentik-uid $authentik_uid;
}

# all requests to /outpost.gauthentik.io must be accessible without authentication
location /outpost.gauthentik.io {
    proxy_pass          http://0.0.0.0:3001/outpost.gauthentik.io;
    # ensure the host of this vserver matches your external URL you've configured
    # in authentik
    proxy_set_header    Host $host;
    proxy_set_header    X-Original-URL $scheme://$http_host$request_uri;
    add_header          Set-Cookie $auth_cookie;
    auth_request_set   $auth_cookie $upstream_http_set_cookie;
    proxy_pass_request_body off;
    proxy_set_header    Content-Length "";
}

# Special location for when the /auth endpoint returns a 401,
# redirect to the /start URL which initiates SSO
location @gauthentik_proxy_signin {
    internal;
    add_header Set-Cookie $auth_cookie;
    return 302 /outpost.gauthentik.io/start?rd=$request_uri;
    # For domain level, use the below error_page to redirect to your authentik server with the full redirect path
    # return 302 https://authentik.company/outpost.gauthentik.io/start?rd=$scheme://$http_host$request_uri;
}

```

Increase buffer size for large headers
This is needed only if you get 'upstream sent too big header while reading response
header from upstream' error when trying to access an application protected by goauthentik
proxy_buffers 8 16k;
proxy_buffer_size 32k;

Make sure not to redirect traffic to a port 4443
port_in_redirect off;

location / {
 # Put your proxy_pass to your application here
 proxy_pass \$forward_scheme://\$server:\$port;
 # Set any other headers your application might need
 # proxy_set_header Host \$host;
 # proxy_set_header ...;

authentik-specific config #####
auth_request /outpost.gauthentik.io/auth/nginx;
error_page 401 = @gauthentik_proxy_signin;
auth_request_set \$auth_cookie \$upstream_http_set_cookie;
add_header Set-Cookie \$auth_cookie;

translate headers from the outposts back to the actual upstream
auth_request_set \$authentik_username \$upstream_http_x_authentik_username;
auth_request_set \$authentik_groups \$upstream_http_x_authentik_groups;
auth_request_set \$authentik_email \$upstream_http_x_authentik_email;
auth_request_set \$authentik_name \$upstream_http_x_authentik_name;
auth_request_set \$authentik_uid \$upstream_http_x_authentik_uid;

proxy_set_header X-authentik-username \$authentik_username;
proxy_set_header X-authentik-groups \$authentik_groups;
proxy_set_header X-authentik-email \$authentik_email;
proxy_set_header X-authentik-name \$authentik_name;
proxy_set_header X-authentik-uid \$authentik_uid;

}

all requests to /outpost.gauthentik.io must be accessible without authentication
location /outpost.gauthentik.io {
 proxy_pass http://0.0.0.0:3001/outpost.gauthentik.io;
 # ensure the host of this vserver matches your external URL you've configured
 # in authentik
 proxy_set_header Host \$host;
 proxy_set_header X-Original-URL \$scheme://\$http_host\$request_uri;
 add_header Set-Cookie \$auth_cookie;
 auth_request_set \$auth_cookie \$upstream_http_set_cookie;
 proxy_pass_request_body off;
 proxy_set_header Content-Length "";

Special location for when the /auth endpoint returns a 401,
redirect to the /start URL which initiates SSO
location @gauthentik_proxy_signin {
 internal;
 add_header Set-Cookie \$auth_cookie;
 return 302 /outpost.gauthentik.io/start?rd=\$request_uri;
 # For domain level, use the below error_page to redirect to your authentik server with the full redirect path
 # return 302 https://authentik.company/outpost.gauthentik.io/start?rd=\$scheme://\$http_host\$request_uri;

Konfiguration der Puffergrößen für den Header mit der Fehlermeldung zu verhindern

Portkonfiguration: Portweiterleitung in URLs ist deaktiviert

Standortkonfiguration mit /location:
mit proxy_pass wird auf die zu schützende Anwendung gesetzt

Authentifizierungsanfrage an den Standort stellen

extrahiert Informationen aus den Antwort-Headern, die vom Authentik-Server erhalten wurden

setzt HTTP-Anfrageheader, die die aus Authentik erhaltenen Informationen enthalten und werden an die Anwendung übergeben

Standortblock für Anfragen an /outpost.gauthentik.io, die direkt zur Authentik Outputs umgeleitet werden und demonstrativ unter der ip 0.0.0.3001 läuft

wenn eine 401 (unbefugt)-Antwort vom Endpunkt empfangen wird, erfolgt eine Weiterleitung zur /start URL

A Anhang

A Anhang

A.11 TOTP-Konfiguration

A.12 Benutzerdokumentation

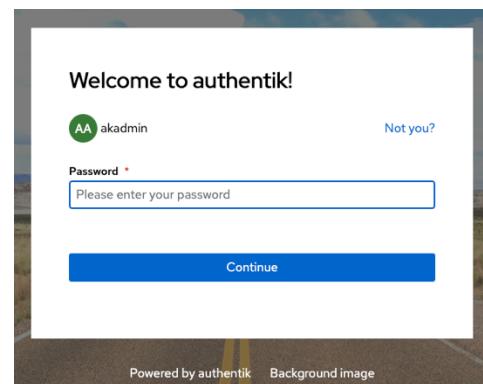
Benutzerdokumentation

AUTHENTIK

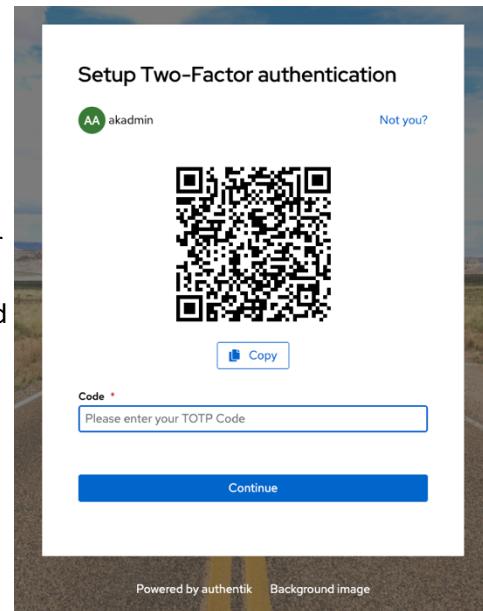
Was ist Authentik?

Authentik ist ein Open-Source-Identity-Provider mit dem Schwerpunkt auf Flexibilität und Vielseitigkeit. Es ist möglich Authentik in einer bestehenden Umgebung verwenden, um Unterstützung für neue Protokolle, Anmeldung/Wiederherstellung/etc. hinzuzufügen.

1. User erhalten Zugangsdaten für Authentik
2. User melden sich mit den Zugangsdaten für Authentik an (siehe Bild rechts)



3. Nach der ersten Anmeldung, werden die User durch einen QR-Code aufgefordert, den Microsoft Authenticator zu nutzen
4. Einen Account im Microsoft Authenticator hinzufügen und QR-Code scannen (rechts ein Bild des QR-Codes)



5. Dashboard, was erscheint, wenn eine direkte Anmeldung bei Authentik und nicht bei anderen Services erscheint

Action	User	Creation Date	Client IP	Tenant
User was written to	akadmin	06/11/2023, 16:13:23	192.168.65.1	Default tenant
Model updated	akadmin	06/11/2023, 16:13:23	192.168.65.1	Default tenant
Model created	akadmin	06/11/2023, 15:50:34	192.168.65.1	Default tenant
Login	akadmin	06/11/2023, 15:49:44	192.168.65.1	Default tenant
User was written to	akadmin	06/11/2023, 15:49:44	192.168.65.1	Default tenant