

Labor-Aufbau für ein Identity und Access Management System und Implementation des Identity Lifecycles

Version 1.0

Autor: Mike Dätwyler

Fachrichtung: Informatiker Systemtechnik EFZ

Dokumentation: Bericht der praktischen Abschlussarbeit

Verantwortliche Fachkraft: Andreas Stadelmann

Verantwortlicher Berufsbildner: Urs Grubenmann

Hauptexperte: Florian Reck

Zweitexperte: Tom Enz

Projekt-Beginn/-Ende: 23.02.2023 – 09.03.2023

Ausbildungsbetrieb: Suva | Rösslimattstrasse 39, 6005 Luzern

Versionsliste

Datum	Version	Kommentar	Autor
23.02.2023	0.1	Dokument initialisiert und Grundinformationen angepasst	Mike Dätwyler
23.02.2023	0.2	PA-Bericht Teil 1 (exkl. Zeitplan/Arbeitsjournal)	Mike Dätwyler
24.02.2023	0.3	Projektbeschreibung	Mike Dätwyler
24.02.2023	0.4	Anforderungsanalyse	Mike Dätwyler
27.02.2023	0.5	Detailkonzept	Mike Dätwyler
01.03.2023	0.6	Benutzeranleitung (Installation/Konfiguration)	Mike Dätwyler
02.03.2023	0.7	Benutzeranleitung (Implementation)	Mike Dätwyler
02.03.2023	0.8	Umsetzung – Bericht	Mike Dätwyler
08.03.2023	0.9	Testing und Schlusswort	Mike Dätwyler
08.03.2023	0.10	Management Summary	Mike Dätwyler
09.03.2023	1.0	Abgabe	Mike Dätwyler

Inhaltsverzeichnis

1	Management Summary	5
1.1	Ausgangssituation.....	5
1.2	Umsetzung	5
1.3	Ergebnis	5
2	PA-Bericht Teil 1.....	6
2.1	Einleitung	6
2.1.1	Zum Dokument.....	6
2.1.2	Themenwahl.....	6
2.1.3	Die Suva	6
2.1.4	Projektaufbauorganisation.....	7
2.1.5	Organisation der Arbeitsergebnisse	7
2.2	Aufgabenstellung und Ausgangslage	8
2.2.1	Ausgangslage	8
2.2.2	Detaillierte Aufgabenstellung.....	8
2.2.3	Identity Lifecycle.....	8
2.2.4	Vorkenntnisse	9
2.2.5	Vorarbeiten.....	9
2.2.6	Benutzte Firmenstandards	9
2.3	Zeitplan	10
2.4	Arbeitsjournal	11
2.4.1	Tag 1: Donnerstag, 23.02.2023.....	11
2.4.2	Tag 2: Freitag, 24.02.2023	12
2.4.3	Tag 3: Montag, 27.02.2023.....	13
2.4.4	Tag 4: Dienstag, 28.02.2023	14
2.4.5	Tag 5: Mittwoch, 01.03.2023.....	15
2.4.6	Tag 6: Donnerstag, 02.03.2023.....	16
2.4.7	Tag 7: Montag, 06.03.2023.....	17
2.4.8	Tag 8: Dienstag, 07.03.2023	18
2.4.9	Tag 9: Mittwoch, 08.03.2023.....	19
2.4.10	Tag 10: Donnerstag, 09.03.2023.....	20
2.4.11	Sprint 1.....	21
2.4.12	Sprint 2.....	22
3	PA-Bericht Teil 2.....	23
3.1	Projektbeschreibung.....	23
3.1.1	Auftrag	23

3.1.2	Abgrenzung.....	23
3.1.3	Systeme	23
3.1.4	Projektmanagementmethode (Scrum).....	23
3.2	Anforderungsanalyse	25
3.2.1	Analyse des Ist-Systems.....	25
3.2.2	Soll-Systembeschreibung.....	26
3.3	Detailkonzept.....	28
3.3.1	Systemlandschaft – Internes IAM.....	28
3.3.2	Failover-Szenarien	29
3.3.3	Benutzeranleitung	29
3.3.4	Identity Lifecycle.....	29
3.3.5	Lösungsvarianten.....	30
3.4	Umsetzung.....	32
3.4.1	Labor-Aufbau	32
3.4.2	Identity Lifecycle.....	36
3.4.3	Sicherheitsaspekte.....	37
3.4.4	Systemarchitektur	38
3.5	Testing.....	39
3.5.1	Testkonzept	39
3.5.2	Testfälle	40
3.5.3	Testprotokoll.....	51
3.5.4	Testresultate.....	52
3.6	Auswertung – Zielkatalog	52
4	Schlusswort	53
	Abkürzungsverzeichnis	54
	Glossar	55
	Literaturverzeichnis	63
	Abbildungsverzeichnis	66
	Anhang	68
	Schedules – Log Files	68
	Datensicherung der Arbeit.....	74
	Jira Software – Scrum Board.....	75
	Floatchart.....	77
	Benutzeranleitung	78
	Besprechungsprotokoll: Expertenbesuch.....	113

1 Management Summary

1.1 Ausgangssituation

Bereits 24 Jahre wendet die Suva Identity & Access Management an. Das Produkt, welches dafür verwendet wird, ist seit 2018 der Identity Manager. Der Produkthersteller ist One Identity und dieser hat im Herbst 2022 einen neuen Release zum Download auf seiner Website zur Verfügung gestellt.

Das Suva-interne Identity & Access Management Team möchte immer anhand einer Out-of-the-box-Installation verschiedene Tests auf neuen Versionen durchführen, bevor eine bestehende Umgebung auf diese upgedatet wird. Zudem soll zusätzlich der Identity Lifecycle nach Suva-Standard implementiert werden.

1.2 Umsetzung

Gleich zu Beginn wurde eine detaillierte Planung erstellt. Die verwendete Projektmanagementmethode «Scrum» wurde ebenfalls gleich angewandt. Die Grundlage dieser Arbeit bietet die Anforderungsanalyse. In dieser ist die Ist-Situation aufgenommen worden. Aus den daraus gewonnenen Erkenntnissen entstand ein Zielkatalog, welcher die Soll-Systembeschreibung definiert.

Im Detailkonzept wurden die Systemumgebung, Benutzeranleitung, Failover-Szenarien und der Identity Lifecycle mit den dazugehörigen Lösungsvarianten ausgearbeitet. Auf dieser Grundlage konnte spezifisch an den Laboraufbau sowie die Implementation herangegangen werden.

Die Installation fand auf einem bestehenden Windows Server statt, auf dem bereits andere Versionen des Identity Managers im Betrieb sind. Als Teil der Konfiguration des Systems wurde ein Job-Service, Config. Parameter und Passwort-Richtlinien konfiguriert. Das Labor wurde auf der Teststufe der Suva, der ENTW, aufgebaut.

Nachdem das Labor komplett einsatzbereit war, ging die Implementation des Identity Lifecycles vonstatten. Dabei wurde die im Detailkonzept gewählte Lösungsvariante, welche den Suva-Standard erfüllt, umgesetzt.

Durch ein anschliessendes Testing konnte bestätigt werden, dass das Labor und der Identity Lifecycle einwandfrei funktionieren.

1.3 Ergebnis

Das Resultat dieser Arbeit ist ein aufgebautes Labor des Identity Managers in der Version 9.1 und darauf der funktionierende Identity Lifecycles. Das Labor wurde nach Suva-Standard installiert und konfiguriert. Der Identity Lifecycle wurde ebenfalls nach Suva-Standard implementiert.

Die dazugehörige Benutzeranleitung ist im Anhang auffindbar. Eine Zusammenfassung dieser sowie eine Abbildung der Systemarchitektur und eine dazugehörige Sicherheitsanalyse findet sich im Bericht der Umsetzung im Kapitel «3.4 Umsetzung».

Des Weiteren wurden alle aktiven Mitarbeiter in die Labor-Umgebung übertragen und ein LDAP Verzeichnis ist angebunden und synchronisiert.

Die zu erreichenden Ziele sind erfolgreich umgesetzt worden. Das Labor und der Identity Lifecycle funktionieren einwandfrei, was bedeutet, dass mit dem System nun ein Testing für die produktiven Systeme durchgeführt werden kann.

2 PA-Bericht Teil 1

2.1 Einleitung

2.1.1 Zum Dokument

Die vorliegende Arbeit beschreibt den genauen Ablauf sowie mein Vorgehen bei meiner PA. Diese wird am Ende der Arbeit zur Prüfung und Bewertung eingereicht. Alle Fachbegriffe und Abkürzungen sind im Abkürzungsverzeichnis bzw. Glossar aufzufinden, welche sich am Ende dieses Dokumentes befinden. Zu den jeweiligen Informationsquellen der Wissensbeschaffung, im Literaturverzeichnis, finden sich Verweise direkt im Text in Form einer Klammer – Zitierweise nach Harvard. Auf erwähnte Unternehmen und Produkte wird jeweils lediglich per Link verwiesen.

2.1.2 Themenwahl

Das Thema IAM wurde gewählt, da ich persönlich Interesse an IAM besitze und es in Zukunft immer wichtiger sein wird. Das IAM-Team der Suva setzt zu jeder neuen Version ihres Tools eine Testumgebung auf. Die Anforderung für eine solche Testumgebung ist nun wieder präsent, da es eine neue Version des Tools gibt. Aus diesem Grund werde ich im Verlauf dieser praktischen Arbeit eine Testumgebung eines IAM-Systems aufsetzen. Zusätzlich werde ich auf dieser noch einen Identity Lifecycle implementieren.

Meiner Meinung nach ist dies eine spannende und lehrreiche Arbeit, welche auch in Zukunft wieder auf mich zukommen könnte. Das sind somit auch schon die ausschlaggebenden Punkte, weshalb ich mich für dieses Thema entschlossen habe.

2.1.3 Die Suva

Die Suva (Schweizerische Unfallversicherungsanstalt) ist der grösste Unfallversicherer der Schweiz. Sie bietet den obligatorischen Versicherungsschutz für Arbeitnehmer und Arbeitslose gegen Unfälle und Berufskrankheiten. Dies entspricht ungefähr 129'000 Unternehmen bzw. 2 Millionen Berufstätige. Seit 2005 führt die Suva im Auftrag des Bundes auch die Militärversicherung. Die Dienstleistungen der Suva umfassen Prävention, Versicherung und Rehabilitation. Sie arbeitet selbsttragend, ohne öffentliche Gelder und gibt Gewinne in Form von tieferen Prämien an die Versicherten zurück. Im Suva-Rat nehmen die Vertreter der Arbeitgeber sowie Arbeitnehmer und die Vertreter und Vertreterinnen des Bundes Einstitz. (Suva, 2022)

In der Abteilung Informatik sind aktuell 352 interne und externe Mitarbeiter beschäftigt (Stand 23.02.2023). Die Abteilung ist in sechs Bereiche unterteilt und diese sind wiederum in mehrere Teams aufgeteilt. Seit dem Sommer 2020 werden jährlich zwei Lernende der Fachrichtung Plattformentwicklung EFZ und gleich vier Lernende der Fachrichtung Applikationsentwicklung EFZ ausgebildet. Aus dem Organigramm der Abteilung Informatik ist ersichtlich, in welchem Bereich und Team ich aktuell aufgestellt bin. Der Bereich «Operation Services» ist quasi der «Hub» der Suva Informatik, bestehend aus vielen verschiedenen Teams. Darunter der Service Desk, der 2nd-Level vor Ort Support oder auch die IT-Security, wo bspw. mein siebenköpfiges Team, das IAM-Team, angesiedelt ist.

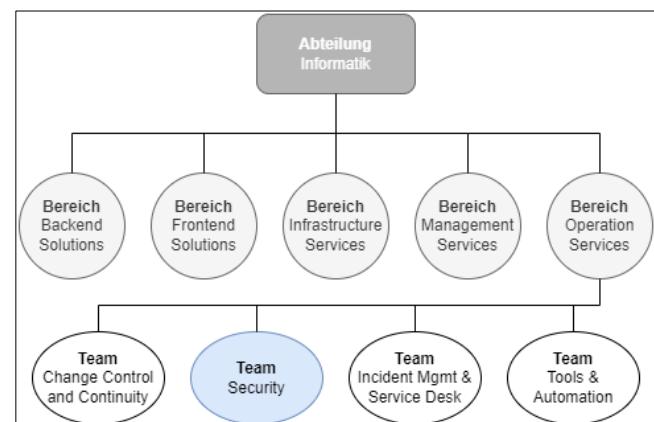


Abbildung 1: Organigramm – Suva Informatik (Dätwyler, 2023)

2.1.4 Projektaufbauorganisation

Folgend werden die involvierten Parteien in Form eines Organigramms aufgezeigt:

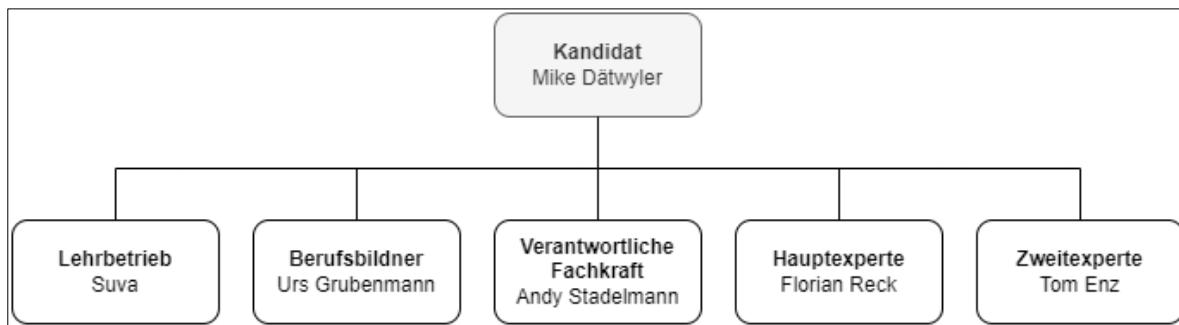


Abbildung 2: Projektaufbauorganisation (Dätwyler, 2023)

2.1.5 Organisation der Arbeitsergebnisse

Alle relevanten Dateien, welche ich in dieser Arbeit verwende, werden im OneDrive gespeichert, wo sie automatisch ständig gesichert und versioniert werden. Zusätzlich werde ich die Dateien täglich auf ein, von der Suva ebenfalls versioniertes, Netzlaufwerk ablegen und sie in mein persönliches Google Drive spiegeln. Die Wiederherstellung gesicherter Arbeitsschritte ist somit gewährleistet.

2.1.5.1 Versionierung

Die Versionierung des Dokumentes wird nach meinem Ermessen und möglichst nach Entwicklungsstand durchgeführt. Dabei achte ich darauf, dass ich nach den meisten grösseren Kapitel eine neue Version ansetze. Wie dies umgesetzt wurde, kann der Versionsliste auf Seite 2 entnommen werden.

Die Versionen werden dann jeweils auf OneDrive, Netzlaufwerk und Google Drive im Ordner «Backup-Archiv» gespeichert. Auf die Arbeitsergebnisse kann somit jederzeit zugriffen werden.

2.1.5.2 Tägliche Sicherung

Um den jeweiligen Tagesfortschritt einzusehen, wird eine tägliche Sicherung in den «Backup-Archiv»-Ordner gespeichert.

→ Screenshots zur Datensicherung finden sich im Anhang.

2.2 Aufgabenstellung und Ausgangslage

2.2.1 Ausgangslage

Die Suva setzt auf Identity & Access Management, genauer, den Identity Manager. Der Hersteller, One Identity, hatte einen neuen Release auf seiner Website veröffentlicht. Bevor die drei Stufen/Umgebungen der Suva upgedatet werden, soll eine Out-of-the-box Version für Testzwecke aufgebaut werden. Diese Testinstallation ermöglicht es dem internen IAM-Team der Suva, die Standard Identity Manager Prozesse in einer separaten Umgebung zu testen.

2.2.2 Detaillierte Aufgabenstellung

Ziel dieser PA ist es, eine Testinstallation des Identity Managers in der aktuellen Version 9.1 auszuführen sowie einen Identity Lifecycle auf dieser zu implementieren. Dies gemäss Suva-Standard.

Nach der Installation soll vom produktiven System ein Export aller aktiven Mitarbeiter ausgeführt werden, dabei ist der Stichtag der Tag der Installation oder der folgende Arbeitstag. Dieser Export soll dann anschliessend ins neu aufgesetzte IAM-System importiert werden. Nachgewiesen werden soll dies mittels eines Reports, in welchem ein Total der Anzahl Mitarbeiter im System angezeigt wird. Weiter soll ein Zielsystem, ein LDAP-Verzeichnis, angeschlossen werden. Alle vorhandenen Accounts sollen dabei initial eingelesen werden. Beim Hinzufügen einer Identität soll ein LDAP Account erstellt werden, bei der Änderung des Nachnamens einer Identität soll diese Änderung bis zum LDAP Account übernommen werden und wenn das Austrittsdatum der Identität dem Tagesdatum gleichgesetzt wird, soll die Identität deaktiviert und der LDAP Account in die verzögerte Löschung aufgenommen werden.

Getestet werden soll, ob die Verarbeitung der eingeplanten Routine Tasks im IAM System fehlerfrei funktioniert. Dies soll mittels Log Files nachgewiesen werden. Weiter ist zu testen, ob der Identity Lifecycle funktioniert.

Es wird zudem erwartet, dass ein Big Picture der Systemarchitektur und eine Benutzeranleitung zur Installation, Konfiguration und Implementation erstellt wird.

2.2.3 Identity Lifecycle

Der Identity Lifecycle dreht sich um drei Prozesse:

Joiner: Ein Mitarbeiter tritt einem Unternehmen bei und wird daher im HCM-System aufgenommen. Von da aus gelangt er dann ins IAM System.

Mover: Der Mitarbeiter wechselt im Verlaufe seiner Amtszeit möglicherweise die Abteilung und nimmt eine andere Funktion wahr. Die Änderung wird im HCM-System vorgenommen und ebenfalls ins IAM System synchronisiert.

Leaver: Schlussendlich verlässt der Mitarbeiter das Unternehmen. Der Austritt wird ins HCM-System aufgenommen und wieder mit dem IAM System synchronisiert.

Durch die Implementation eines Identity Lifecycles im IAM System werden beim Joiner automatisch die benötigten Berechtigungen und Konten erteilt. Die Änderungen beim Mover werden ebenfalls automatisiert ausgeführt und beim Leaver werden wieder automatisch alle Berechtigungen und Konten entzogen, bevor die Identität deaktiviert/gelöscht wird. Durch den Identity Lifecycle verhindert man also «Account-Leichen» und erhält einen Automatismus.

2.2.3.1 Lösungsvarianten

Um den Identity Lifecycle zu implementieren, muss ich mich für eine Implementationsvariante entscheiden. Im Identity Manager gibt es vier Varianten wie man einen Identity Lifecycle implementieren kann, diese wären:

1. Manuelle Zuteilung
2. Account Definition
3. Account Definition mit Department
4. Account Definition mit Geschäftsrolle

In der Suva wenden wir hauptsächlich die zweite Variante an.

Eine genauere Beschreibung der Lösungsvarianten sowie die begründete Entscheidung zu meiner gewählten Lösungsvariante erläutere ich im Kapitel «3.3 Detailkonzept».

2.2.4 Vorkenntnisse

- Allgemeine Kenntnisse über die Suva Server- und Netzwerkinfrastruktur aus dem betrieblichen Alltag und dem Schulunterricht
- Erstellung von Dokumentationen und Anleitungen für den betrieblichen Gebrauch
- Arbeiten mit dem Identity Manager
 - Lernmodul
 - Betriebliche Unterstützung
- Installation und Update bestehender Suva IAM Systeme

2.2.5 Vorarbeiten

- Für die Testinstallation voraussichtlich benötigte Infrastruktur und Berechtigungen vorbereiten
- Download der aktuellen Version vom [Identity Manager \(9.1\)](#)
- Download von [Microsoft .NET 4.8](#)
- Download von [Microsoft Edge WebView2](#)
- Studieren von internen und externen Dokumentationen zum Identity Manager
- Aufsetzung eines Kanban-Boards für Scrum
- Datenbankbestellung bei einem Suva Datenbank Administrator

2.2.6 Benutzte Firmenstandards

- Dokumentenvorlage PA (Anpassungen vorgenommen)
- Vorlage für die Zeitplanung (Anpassungen vorgenommen)

Bei der Arbeit sollen zusätzlich gewisse Firmenstandards eingehalten werden, wie beispielsweise bei der Anbindung des LDAP-Zielsystems.

2.3 Zeitplan

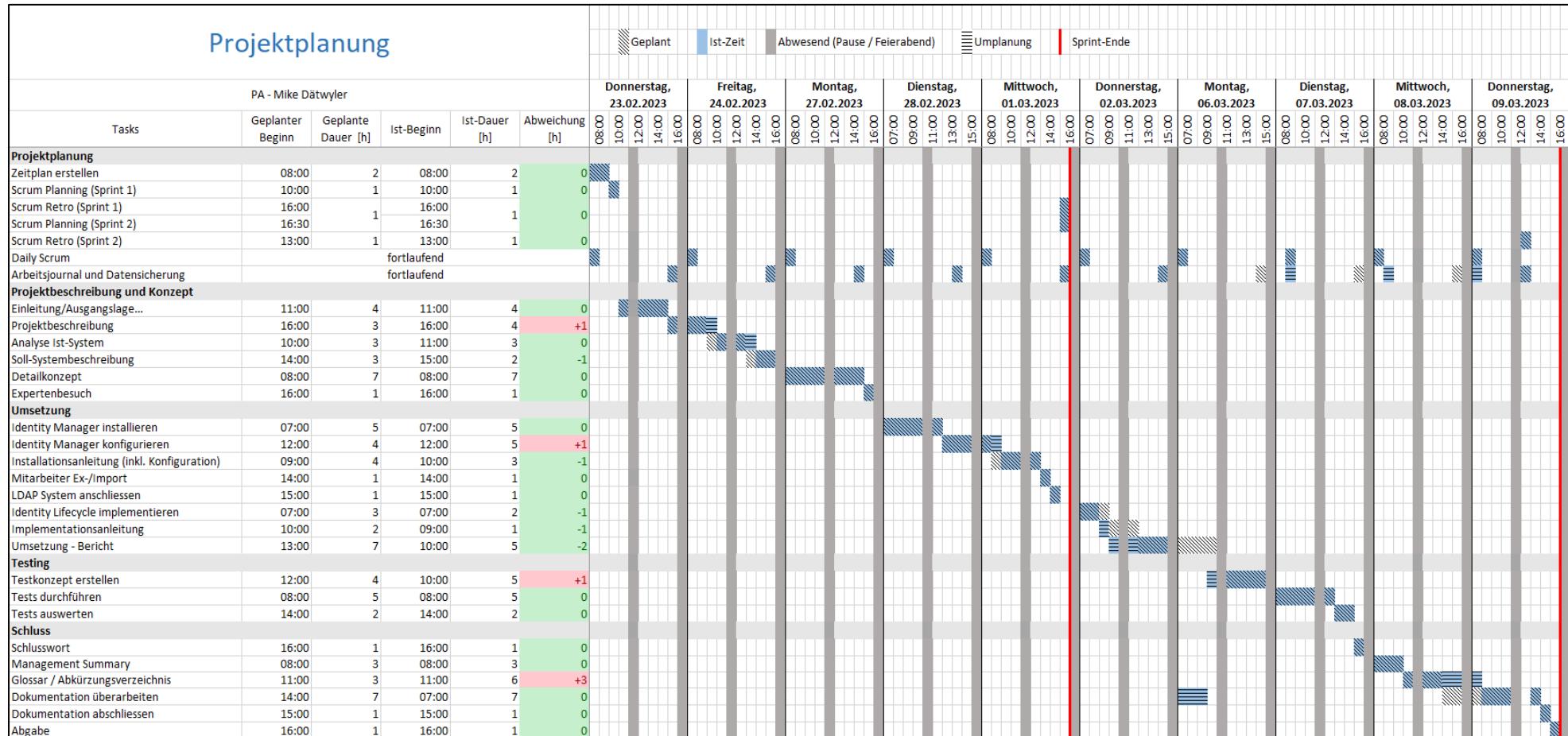


Abbildung 3: Zeitplan (Dätwyler, 2023)

2.4 Arbeitsjournal

Dieses Arbeitsjournal zeigt meine Aufgaben für jeden Tag auf und eine kurze Zusammenfassung, wie mir diese jeweils ergangen sind.

2.4.1 Tag 1: Donnerstag, 23.02.2023

2.4.1.1 Arbeitsrapport

Tasks	Soll [h]	Ist [h]	Abweichung [h]	Restzeit [h]
Zeitplan erstellen	2	2	0	78
Scrum Planning (Sprint 1)	1	1	0	77
Einleitung / Ausgangslage	4	4	0	73
Projektbeschreib	1	1	0	72

Abbildung 4: Arbeitsrapport – 23.02.2023 (Dätwyler, 2023)

2.4.1.2 Daily Scrum

An meinem heutigen Daily konnte ich mir lediglich ein Tagesziel setzen, da heute der erste Tag ist, an dem in an dieser PA arbeite. Ich plante also heute eine präzise Planung aufzustellen.

2.4.1.3 Backup

Ich habe die aktuellen Dokumente gemäss Backup-Konzept ins Netzlaufwerk und in mein Google Drive gespiegelt. Die Version für den heutigen Tag sowie die ersten zwei Versionen wurden ebenfalls zusätzlich abgelegt.

2.4.1.4 Erhaltene Hilfe

Ich konnte beim Zeitplan eine Vorlage benutzen, wodurch ich nicht unnötig Zeit verlor. Dies ist auch im Kapitel «2.2.6 Benutzte Firmenstandards» beschrieben.

2.4.1.5 Erfolge

Ich habe den detaillierten, hoffentlich meist akkurate, Zeitplan erstellt. Ich konnte zudem bereits die Aufgabenstellung spezifischer analysieren und ein paar Lösungsvarianten notieren.

2.4.1.6 Misserfolge oder Probleme

Heute stiess ich auf keine Probleme und hatte keine Misserfolge.

2.4.1.7 Reflexion

Ich konnte für den ersten Tag bereits viel erledigen. Mit meinem Vorgehen war ich so weit zufrieden, da ich stets der, von mir erstellen, Planung gefolgt bin.

Ich habe mir mit der Planung extra etwas Zeit genommen, damit ich die nächsten Tage eine gute Basis bzw. Sicherheit habe, um dann den Rest der Arbeit erfolgreich zu erledigen. Meinen ersten Sprint konnte ich bereits planen und auch gleich starten.

Ich werde morgen mit einem guten Gefühl in den Tag starten.

2.4.2 Tag 2: Freitag, 24.02.2023

2.4.2.1 Arbeitsrapport

Tasks	Soll [h]	Ist [h]	Abweichung [h]	Restzeit [h]
Projektbeschreibung	2	3	+1	69
Analyse Ist-System	3	3	0	66
Soll-Systembeschreibung	3	2	-1	64

Abbildung 5: Arbeitsrapport – 24.02.2023 (Dätwyler, 2023)

2.4.2.2 Daily Scrum

Gestern konnte ich einen Zeitplan erstellen, einen Sprint starten und die Ein-/Ausgangslage schreiben.

Heute möchte ich die Projektbeschreibung und die Anforderungsanalyse fertigstellen.

2.4.2.3 Backup

Ich habe erneut die aktuellen Dokumente gemäss Backup-Konzept ins Netzlaufwerk und in mein Google Drive gespiegelt. Die Version für den heutigen Tag wurde ebenfalls abgelegt.

2.4.2.4 Erhaltene Hilfe

Bei den Kann-Kriterien der Soll-Systembeschreibung versuchte mich Andy Stadelmann, mein Praxisbildner, ein wenig in die richtige Richtung zu lenken. Ich sollte darüber nachdenken, was ich grundsätzlich nicht einrichten würde oder wovon ich vielleicht nicht gleich viel installiere wie in den produktiven Systemen. Ich fragte ihn dazu bereits gestern, da ich mir da schon Gedanken dazu gemacht hatte.

2.4.2.5 Erfolge

Dank des gestrigen Denkanstosses durch Andy Stadelmann kam ich schlussendlich doch noch eine Idee für zwei Kann-Kriterien.

2.4.2.6 Misserfolge oder Probleme

Ich habe den Zweitaufwand für die Projektbeschreibung ein wenig falsch eingeschätzt.

2.4.2.7 Reflexion

Ich konnte heute bereits mit der Anforderungsanalyse starten und konnte die Soll-Systembeschreibung schneller abschliessen als gedacht. So konnte ich die verlorene Zeit bei der Projektbeschreibung gleich wieder aufholen.

Die Planung, welche ich gestern erstellt habe, half mir heute dabei, strukturiert an der Arbeit tätig zu sein.

Ich kann auch heute guten Gewissens in den Feierabend gehen und am Montag wieder motiviert starten.

2.4.3 Tag 3: Montag, 27.02.2023

2.4.3.1 Arbeitsrapport

Tasks	Soll [h]	Ist [h]	Abweichung [h]	Restzeit [h]
Detailkonzept	7	7	0	57
Expertenbesuch	1	1	0	56

Abbildung 6: Arbeitsrapport – 27.02.2023 (Dätwyler, 2023)

2.4.3.2 Daily Scrum

Am Freitag konnte ich die Projektbeschreibung und die Anforderungsanalyse fertigstellen.

Heute möchte ich das Detailkonzept abschliessen können.

2.4.3.3 Backup

Ich habe die aktuellen Dokumente gemäss Backup-Konzept ins Netzlaufwerk und in mein Google Drive gespiegelt. Die Version für den heutigen Tag wurde ebenfalls zusätzlich abgelegt.

2.4.3.4 Erhaltene Hilfe

Bei der Kreierung des Big Pictures warf ich einen Blick auf unsere internen Dokumente, welche die Systemlandschaft/-architektur behandeln.

2.4.3.5 Erfolge

Ich konnte das Detailkonzept abschliessen.

2.4.3.6 Misserfolge oder Probleme

Ich hatte ein bisschen Probleme damit, mich korrekt an die verschiedenen Varianten, wie der Identity Lifecycle implementiert werden kann, zu erinnern und vor allem deren Funktionsweise.

2.4.3.7 Reflexion

Ich konnte mich heute sehr gut auf das Detailkonzept konzentrieren, da ich mich immer wieder in einen Tunnelmodus begehen konnte. Ich fand es schwierig abzuschätzen, was genau alles ins Detailkonzept gehört und in welchem Volumen. Persönlich bin ich stolz auf meine Big Picture-Zeichnung, da ich finde, dass sie mir gut gelungen ist.

In meinem Scrum-Board war es mir möglich, schon einige Stories auf «done» zu setzen. Morgen kann ich dann bereits «Identity Manager installieren» auf «in progress» setzen.

Da ich momentan keine Abweichung in der Planung habe, fühle ich mich nicht sehr gestresst und nehme mich der Installation am morgigen Tag voller Elan an.

2.4.4 Tag 4: Dienstag, 28.02.2023

2.4.4.1 Arbeitsrapport

Tasks	Soll [h]	Ist [h]	Abweichung [h]	Restzeit [h]
Identity Manager installieren	5	5	0	51
Identity Manager konfigurieren	3	3	0	48

Abbildung 7: Arbeitsrapport – 28.02.2023 (Dätwyler, 2023)

2.4.4.2 Daily Scrum

Gestern konnte ich das Detailkonzept erfolgreich abschliessen.

Mein heutiges Ziel ist es, den Identity Manager zu installieren und mit der Konfiguration zu beginnen.

Gestern hatte ich ein bisschen Probleme damit, mich aufs neue Kapitel einzulassen. Ich denke aber, dass mich dieses Problem heute nicht grossartig hindern wird.

2.4.4.3 Backup

Ich habe erneut die aktuellen Dokumente gemäss Backup-Konzept ins Netzlaufwerk und in mein Google Drive gespiegelt. Die Version für den heutigen Tag wurde ebenfalls zusätzlich abgelegt.

2.4.4.4 Erhaltene Hilfe

Bei der Installation gab es ein paar Neuerungen, welche in der vorhandenen internen Dokumentation nicht enthalten waren. Dafür konsultierte ich Andy Stadelmann.

2.4.4.5 Erfolge

Ich konnte die Installation erfolgreich abschliessen.

2.4.4.6 Misserfolge oder Probleme

Es tauchten ein paar Unklarheiten bei der Installation auf, da die neue Version ein paar Neuerungen mit sich gebracht hat. Die Reihenfolge der Konfiguration war etwas wirr, weshalb ich dadurch etwas Zeit verlor.

2.4.4.7 Reflexion

Bei der Konfiguration war die Reihenfolge meiner Schritte ein bisschen chaotisch, wodurch ich beinahe viel Zeit verlor. Ich konnte mich jedoch trotzdem noch an den Zeitplan halten.

Ich hätte hierbei meine Herangehensweise überdenken sollen. Hätte ich etwas mehr vorausgedacht, hätte ich wahrscheinlich weniger Zeit dafür benötigt.

Ich werde das meinem morgigen Scrum Daily aufnehmen und nochmals reflektieren.

2.4.5 Tag 5: Mittwoch, 01.03.2023

2.4.5.1 Arbeitsrapport

Tasks	Soll [h]	Ist [h]	Abweichung [h]	Restzeit [h]
Identity Manager konfigurieren	1	2	+1	46
Installationsanleitung (inkl. Konfiguration)	4	3	-1	43
Mitarbeiter Ex-/Import	1	1	0	42
LDAP Anschliessen	1	1	0	41
Scrum Retro (Sprint 1)	0.5	0.5	0	40.5
Scrum Planning (Sprint 2)	0.5	0.5	0	40

Abbildung 8: Arbeitsrapport – 01.03.2023 (Dätwyler, 2023)

2.4.5.2 Daily Scrum

Am gestrigen Tag installierte ich den Identity Manager und begann mit der Konfiguration.

Heute möchte ich die Installationsanleitung fertigstellen und den Mitarbeiter Ex-/Import durchführen. Danach soll noch das LDAP angeschlossen werden und ich werde ein Retro/Planning durchführen.

Gestern hat mich ein Mangel von Vorausdenken gehindert – das wird heute nicht mehr vorkommen.

2.4.5.3 Backup

Auch heute habe ich die aktuellen Dokumente gemäss Backup-Konzept ins Netzlaufwerk und in mein Google Drive gespiegelt. Die Version für den heutigen Tag wurde ebenfalls zusätzlich abgelegt.

2.4.5.4 Erhaltene Hilfe

Heute machte ich Gebrauch von der internen Dokumentation der bei uns in der Suva im IAM-System gesetzten Configuration Parameter (Dätwyler, 2022). Zudem warf ich noch einen Blick auf die Security-Richtlinien-Dokumentation (Stadelmann, 2023), welche ich für die Konfiguration der Passwort-Richtlinien verwendete.

2.4.5.5 Erfolge

Ich konnte die Konfiguration und den Grossteil der Benutzeranleitung fertigstellen. Zudem konnte ich alle aktiven Mitarbeiter sowie die vorhandenen LDAP-Accounts importieren.

2.4.5.6 Misserfolge oder Probleme

Heute konnte ich keine Misserfolge oder Probleme feststellen.

2.4.5.7 Reflexion

Heute kam ich gut voran. Ich konnte die Arbeitsschritte gemäss Arbeitsplanung ausführen, trotz zweier Abweichungen. Morgen kann ich nun somit mit der Implementation des Identity Lifecycles starten. Ich habe heute den ersten von 2 Sprints in dieser PA abgeschlossen, ein Retro durchgeführt und gleich danach noch den zweiten Sprint, in Form eines Scrum-Plannings, geplant.

2.4.6 Tag 6: Donnerstag, 02.03.2023

2.4.6.1 Arbeitsrapport

Tasks	Soll [h]	Ist [h]	Abweichung [h]	Restzeit [h]
Identity Lifecycle implementieren	3	2	-1	38
Implementationsanleitung	2	1	-1	37
Umsetzung – Bericht	3	5	+2	32

Abbildung 9: Arbeitsrapport – 02.03.2023 (Dätwyler, 2023)

2.4.6.2 Daily Scrum

Gestern konnte ich die Konfiguration des Identity Managers, ein grosser Teil der Benutzeranleitung und den Import von Mitarbeiter und Accounts erledigen.

Am heutigen Tag werde ich mich der Implementation des Identity Lifecycles und der Anleitung dazu, wie auch dem Bericht der Umsetzung widmen.

2.4.6.3 Backup

Ich habe die aktuellen Dokumente gemäss Backup-Konzept ins Netzlaufwerk und in mein Google Drive gespiegelt. Die Version für den heutigen Tag wurde ebenfalls zusätzlich abgelegt.

2.4.6.4 Erhaltene Hilfe

Heute musste ich keine Hilfe in Anspruch nehmen.

2.4.6.5 Erfolge

Ich fand trotz minimalen Anfangsschwierigkeiten noch Anklang beim Bericht der Umsetzung.

2.4.6.6 Misserfolge oder Probleme

Heute stiess ich auf keine Probleme oder Misserfolge.

2.4.6.7 Reflexion

Ich konnte heute sehr produktiv in meinen zweiten Sprint starten. Da ich für die Implementation weniger Zeit als geplant benötigt habe, konnte ich den Bericht der Umsetzung bereits fertig schreiben.

Heute hat mich überrascht, dass ich den Identity Lifecycle und die entsprechende Benutzeranleitung viel schneller erarbeiten konnte als geplant.

Ich gehe davon aus, dass mir die Vorsätze aus dem gestrigen Retro stark dabei geholfen haben, heute so effizient an der PA zu arbeiten.

2.4.7 Tag 7: Montag, 06.03.2023

2.4.7.1 Arbeitsrapport

Tasks	Soll [h]	Ist [h]	Abweichung [h]	Restzeit [h]
Dokumentation überarbeiten	0	3	+3	29
Testkonzept erstellen	4	5	+1	24

Abbildung 10: Arbeitsrapport – 06.03.2023 (Dätwyler, 2023)

2.4.7.2 Daily Scrum

Letzten Donnerstag konnte ich den Identity Lifecycle erfolgreich implementieren und die entsprechende Benutzeranleitung dazu verfassen. Den Bericht der Umsetzung stellte ich ebenfalls fertig.

Heute möchte ich das Testkonzept schreiben und möglicherweise bereits anfangen Tests durchzuführen.

2.4.7.3 Backup

Auch heute habe ich die aktuellen Dokumente gemäss Backup-Konzept ins Netzlaufwerk und in mein Google Drive gespiegelt. Die Version für den heutigen Tag wurde ebenfalls zusätzlich abgelegt.

2.4.7.4 Erhaltene Hilfe

Heute benötigte ich keinerlei Hilfe.

2.4.7.5 Erfolge

Die Erarbeitung eines präzisen Testkonzepts.

2.4.7.6 Misserfolge oder Probleme

Heute stiess ich auf keine Probleme und hatte keine Misserfolge.

2.4.7.7 Reflexion

Da ich für die Implementation des Identity Lifecycles gestern weniger Zeit benötigte als angedacht, konnte ich den Bericht der Umsetzung bereits fertigstellen und hatte somit heute bereits Zeit damit anzufangen, meine Dokumentation zu überarbeiten. Für das Testkonzept benötigte ich eine Stunde mehr als geplant, was aber kein Hindernis für diese praktische Arbeit ist – ich bin immer noch sehr gut im Zeitplan.

Das von mir erstellte Testkonzept ist mir meiner Meinung nach sehr gelungen. Es ist präzise und enthält viele Informationen. Wie gut es wirklich ist, sehe ich spätestens morgen, wenn ich die Testfälle durchspiele.

Morgen werde ich voraussichtlich das Testing beenden können, um dann schon bald zu einem Schlussspurt des Projektes zu kommen.

2.4.8 Tag 8: Dienstag, 07.03.2023

2.4.8.1 Arbeitsrapport

Tasks	Soll [h]	Ist [h]	Abweichung [h]	Restzeit [h]
Tests durchführen	5	5	0	19
Tests auswerten	2	2	0	17
Schlusswort	1	1	0	16

Abbildung 11: Arbeitsrapport – 07.03.2023 (Dätwyler, 2023)

2.4.8.2 Daily Scrum

Gestern konnte ich das Testkonzept fertigstellen und bereits meine Dokumentation überarbeiten.

Heute möchte ich das Testing beenden und das Schlusswort verfassen.

2.4.8.3 Backup

Heute habe ich die aktuellen Dokumente gemäss Backup-Konzept ins Netzlaufwerk und in mein Google Drive gespiegelt. Die Version für den heutigen Tag wurde ebenfalls zusätzlich abgelegt.

2.4.8.4 Erhaltene Hilfe

Heute musste ich keinerlei Hilfe in Anspruch nehmen.

2.4.8.5 Erfolge

Ich konnte mein Testing erfolgreich beenden.

2.4.8.6 Misserfolge oder Probleme

Es gab heute keine Misserfolge oder Probleme.

2.4.8.7 Reflexion

Das Testing konnte ich heute wie erwartet erfolgreich beenden. Die Auswertung meiner gesetzten Ziele erledigte ich ebenfalls gleich in der Story «Tests auswerten». Dies konnte ich höchst erfreulich erledigen, da ich alle gesetzten Ziele, mit Ausnahme der Kann-Ziele, erreichen konnte.

Mit meinem verfassten Schlusswort bin ich sehr zufrieden. Es war für mich nicht sehr schwierig dieses zu schreiben, da ich bereits durch die IDPA der Berufsmatura darin geübt war.

2.4.9 Tag 9: Mittwoch, 08.03.2023

2.4.9.1 Arbeitsrapport

Tasks	Soll [h]	Ist [h]	Abweichung [h]	Restzeit [h]
Management Summary	3	3	0	13
Glossar / Abkürzungsverzeichnis	3	5	+2	8
Dokumentation überarbeiten	2	0	-2	8

Abbildung 12: Arbeitsrapport – 08.03.2023 (Dätwyler, 2023)

2.4.9.2 Daily Scrum

Am gestrigen Tag konnte ich das Testing mit der Durchführung und dem Entwerten der Ergebnisse erfolgreich beenden. Zudem schrieb ich noch das Schlusswort.

Heute möchte ich die Management Summary und das Glossar respektive Abkürzungsverzeichnis fertigstellen und die Dokumentation weiter überarbeiten.

2.4.9.3 Backup

Zum zweitletzten Mal habe ich heute die aktuellen Dokumente gemäss Backup-Konzept ins Netzlaufwerk und in mein Google Drive gespiegelt. Die Version für den heutigen Tag wurde ebenfalls zusätzlich abgelegt.

2.4.9.4 Erhaltene Hilfe

Ich benötigte heute keine Hilfe.

2.4.9.5 Erfolge

Heute konnte ich die Management Summary abschliessen.

2.4.9.6 Misserfolge oder Probleme

Misserfolge oder Probleme kamen nicht auf.

2.4.9.7 Reflexion

Ich habe heute etwas länger fürs Glossar gebraucht, als ich dachte. Auch wenn ich morgen zusätzlich ungefähr eine Stunde dafür brauche, bin ich trotzdem noch gut im Zeitplan. Die Dokumentation ist nun inhaltlich fast vollständig beendet. Jetzt gilt es diese optimal zu überarbeiten und ihr den nötigen Feinschliff zu verpassen.

Ich bin nun gut vorbereitet, um morgen diese Projektarbeit beenden zu können. Zumindest den grössten Teil davon, denn die Präsentation wartet noch auf mich.

2.4.10 Tag 10: Donnerstag, 09.03.2023

2.4.10.1 Arbeitsrapport

Tasks	Soll [h]	Ist [h]	Abweichung [h]	Restzeit [h]
Glossar / Abkürzungsverzeichnis	0	1	+1	7
Dokumentation überarbeiten	7	4	-3	3
Scrum Retro (Sprint 2)	1	1	0	2
Dokumentation abschliessen	1	1	0	1
Abgabe	1	1	0	0

Abbildung 13: Arbeitsrapport – 09.03.2023 (Dätwyler, 2023)

2.4.10.2 Daily Scrum

Ich konnte gestern die Management Summary und das Glossar/Abkürzungsverzeichnis fertigstellen.

Heute werde ich die Dokumentation final überarbeiten und abschliessen. Zudem werde ich noch ein Retro zum zweiten Sprint dieser Arbeit durchführen.

2.4.10.3 Backup

Zum letzten Mal habe ich heute die aktuellen Dokumente gemäss Backup-Konzept ins Netzlaufwerk und in mein Google Drive gespiegelt. Die Version für den heutigen Tag habe ich ebenfalls zusätzlich abgelegt.

2.4.10.4 Erhaltene Hilfe

Ich benötigte heute keine Hilfe.

2.4.10.5 Erfolge

Ich habe diese Dokumentation fertiggestellt und bin mit ihr zufrieden. Weiter konnte ich den zweiten Sprint beenden und ein wertvolles Retro durchführen.

2.4.10.6 Misserfolge oder Probleme

Heute konnte ich keine Misserfolge oder Probleme feststellen.

2.4.10.7 Reflexion

Am heutigen Tag ging es darum, den Feinschliff der Dokumentation zu erledigen. Ich korrigierte das ganze Dokument nochmals auf Grammatik, Stil und Rechtschreibung. Ich nahm dann zusätzlich noch die Formatierung ein wenig unter die Lupe.

Ich führte ein kurzes Retro durch, um den zweiten Sprint offiziell abzuschliessen.

Jetzt bin ich bereit zur Abgabe.

2.4.11 Sprint 1

2.4.11.1 Planning

Für die Planung des ersten Sprints begab ich mich als Erstes auf mein aufgesetztes Scrum Board. Dort erfasste ich im Product backlog User Stories auf Grundlage des Zeitplans, bei welchen ich den Aufwand nach Story Points schätzte. Die User Stories Ich erstellte danach den eigentlichen Sprint und fügte die User Stories priorisiert nach Zeitplan hinzu. In den einzelnen Stories schrieb ich jeweils Akzeptanzkriterien hinein. Nun konnte ich den Sprint starten.

2.4.11.2 Retro

Im Scrum Board habe ich den Sprint beendet. Ich musste keine User Stories in den nächsten Sprint übernehmen. Einzig den Epic habe ich transferiert.

2.4.11.2.1 Daten sammeln

Bis jetzt finde ich diese PA ein sehr spannendes Erlebnis, auch wenn es ziemlich stressbehaftet ist.

2.4.11.2.2 Erkenntnisse gewinnen

Ich hatte manchmal Schwierigkeiten damit, mein Wissen bei bestimmten Themen wieder aufzufrischen, um somit die jeweils korrekte Methodik anzuwenden. Daraus zieh ich, dass ich versuchen muss etwas vorausschauender und möglicherweise bedachter an der PA zu arbeiten. Was es in dieser PA noch zu tun gibt ist mir jedoch klar, da gibt es keine Verwirrung.

2.4.11.2.3 Massnahmen

KEEP: Ich muss weiterhin fokussiert und konzentriert an der PA arbeiten.

DROP: Im nächsten Sprint möchte ich mich nicht mehr unbedacht in neue Kapitel stürzen.

ADD: Bevor ich ein neues Kapitel angehe, mache ich mir zuerst im Kopf Gedanken dazu.

2.4.11.2.4 Abschluss

Bei meiner nächsten Retrospektive werde ich wieder meine Erkenntnisse festhalten, jedoch möglicherweise ein wenig ausführlicher.

2.4.12 Sprint 2

2.4.12.1 Planning

Ich habe den zweiten Sprint wieder in meinem Scrum Board geplant, indem ich wieder User Stories auf Grundlage des Zeitplans erfasste. Nachdem ich den eigentlichen Sprint erstellt hatte, priorisierte ich die User Stories im Sprint und startete ihn anschliessend.

2.4.12.2 Retro

Auch nach diesem zweiten Sprint müssen keine User Stories übertragen werden, denn ich konnte alles abschliessen. Dieses Mal sogar inklusive Epic. Den Sprint-Abschluss führte ich wieder in meinem aufgesetzten Scrum Board aus.

2.4.12.2.1 Daten sammeln

Auch in diesem zweiten Sprint blieb es spannend. Eine gewisse Anstrengung war jedoch auch hier spürbar. Je näher das Sprint-Ende kam, desto nervöser wurde ich. Denn ich wusste, dass das bedeutet, dass diese PA bald ein Ende findet.

2.4.12.2.2 Erkenntnisse gewinnen

Die bedachtere Herangehensweise konnte ich in diesem Sprint umsetzen, was sich auch bemerkbar machte.

Grossartig schiefgegangen ist nichts. Ich konnte den zweiten Sprint ohne methodische Schwierigkeiten bewältigen, wobei das Retro des ersten Sprints sicherlich geholfen hat.

Es besteht meinerseits keinerlei Verwirrung – ich weiss, was nach dieser Dokumentation ansteht: die Präsentation inklusive Demo und Fachgespräch.

2.4.12.2.3 Massnahmen

KEEP: Auf meinem weiteren Weg muss ich mir weiterhin immer zuerst im Kopf Gedanken zu komplexen Aufgaben machen.

DROP: In zukünftigen Arbeiten könnte ich etwas mehr fortlaufend die Arbeit verbessern.

ADD: Ich möchte mich nicht mehr von Dingen, wie die Formatierung während des Schreibens anzupassen, ablenken lassen.

2.4.12.2.4 Abschluss

Dieses Kapitel mit Inhalt zu beschreiben wäre sinnbefreit, da es in dieser Arbeit keine nächste Retrospektive geben wird. Ein emotionaler Rückblick auf die Retrospektive

3 PA-Bericht Teil 2

3.1 Projektbeschreibung

3.1.1 Auftrag

Im Rahmen dieser PA soll ein Labor für eine Testumgebung aufgebaut werden, in welcher das Standard-Suva-Tool für das Identity & Access Management System installiert und initial konfiguriert wird. Dies soll die aktuelle Version 9.1 sein. Dabei sollen alle aktiven Mitarbeiter mittels einer CSV-Datei (Stichtag = Folge-/Tag der Installation) initial in das Testsystem eingelesen und ein bestehendes LDAP Verzeichnis angebunden werden. Nach erfolgreicher Installation und Konfiguration soll zudem der Identity Lifecycle implementiert werden.

Die ganze Umsetzung soll in einem Bericht festgehalten werden und die Installation, Konfiguration und Implementation wird zusätzlich Schritt-für-Schritt in einer Benutzeranleitung festgehalten.

Weiter soll das Labor und der Identity Lifecycle auf Funktionalität getestet werden.

3.1.2 Abgrenzung

Das Aufsetzen der Windows- und MS SQL Server ist nicht Teil dieser PA, ebenso wenig wie die Aufsetzung einer VDI. Die Netzwerkkonfiguration/-segmentation ist ebenfalls nicht Teil dieser PA, denn dabei wird auf die bereits vorhandene Infrastruktur der Suva zurückgegriffen. Die Testumgebung befindet sich auf der Segmentierungsstufe ENTW, weshalb die Stufe INTG und PROD in dieser Arbeit nicht berücksichtigt werden. Jegliche Mitarbeiter-Mutationen oder Ein-/Austritte nach dem Stichtag werden nicht mehr berücksichtigt. Das Einrichten eines LDAP-Verzeichnisses wird ebenfalls nicht Inhalt dieser PA sein.

3.1.3 Systeme

Alle Systeme und Stufen innerhalb der Suva-Infrastruktur stehen mir zur Verfügung. Speziell, die im Auftrag erwähnte Labor-Umgebung. Ich kann in dieser praktischen Arbeit also auf Ressourcen wie bspw. unsere JumpVDI oder unser produktives IAM System zurückgreifen.

Für den Aufbau des Labors werden bestehende Microsoft Server benutzt.

3.1.4 Projektmanagementmethode (Scrum)

Scrum ist eine Methode, die dabei hilft, auf einer relativ einfachen Art und Weise mit komplexen Prozessen innerhalb eines Projektes umzugehen. Bspw. kann es einem Team dabei helfen, komplexe Produkte zu entwickeln. Bei Scrum findet nicht erst am Ende ein lessons-learned statt, sondern es werden regelmäßig, während der Entwicklung, aus den Reviews Schlüsse gezogen.

3.1.4.1 Scrum-Prinzip: Ablauf

Der Product Owner erfasst User Stories und priorisiert diese. Gemeinsam mit dem ausführenden Team wird dann der nächste Sprint geplant.

Während des Sprints trifft das Team sich einmal pro Tag fürs Daily Scrum. Der Scrum Master coacht während des ganzen Prozesses das Team in Bezug auf Scrum und unterstützt den Product Owner gegebenenfalls.

Am Ende des Sprints werden die Ergebnisse in einem Review durch das Team vorgestellt. Danach reflektiert das Team ihre Vorgehensweise während des Sprints in einem Retro.

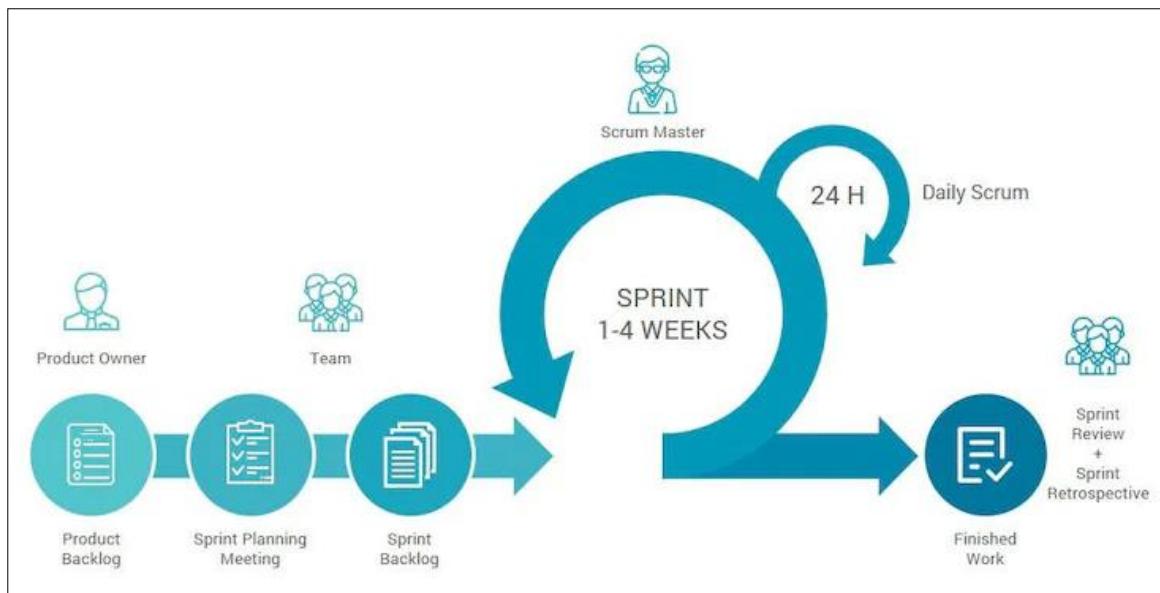


Abbildung 14: Scrum Prinzip (habr.com, 2022)

3.1.4.2 Persönlicher Bezug

Wir setzen bei uns in der Suva seit dem 17. Dezember 2018 auf SAFe, worin wir Scrum als Projektmanagementmethode anwenden. Somit ist Scrum ein wesentlicher Bestandteil meines Alltags. Jedes Team in der Suva Informatik konnte sich bei der Einführung von SAFe einen individuellen Namen aussuchen. Diese insgesamt 42 Teams befinden sich dann jeweils in einem ART. Ab diesem Jahr haben nicht mehr wie bisher drei, sondern gleich fünf ARTs. Ich befinde mich als Mitglied des IAM-Teams, im Team «Gatekeeper», welches sich im ART «Next Suva» befindet.

Da ich die Arbeitsweise nach Scrum als effektiv empfinde und sie mir bereits vertraut ist, habe ich mich für diese Projektmanagementmethode entschieden.

3.1.4.3 Meine Umsetzung

Ich habe mit der Hilfe von Atlassians Jira Software ein Scrum-Board erstellt (siehe Anhang), welches ich meinen Bedürfnissen entsprechend konfiguriert habe. Auf diesem Board erstellte ich dann einen Epic «Projektarbeit» und daran angefügt sind meine User Stories. Diese sind alle jeweils nach Story Points geschätzt. Die Dauer eines Story Points kann selbst definiert werden – ich definiere 1 Story Point = 2 Stunden.

Da ich diese Arbeit allein schreibe, wird die Rolle des Scrum Masters nicht benötigt, da es kein Team gibt, dass gecoacht werden muss. Dafür werde ich die Rolle des Product Owners übernehmen, denn ich bin dafür zuständig, das Product backlog zu verwalten.

Ich werde mit zwei Sprints arbeiten, welche jeweils 1 Woche dauern. Nach dem Start eines Sprints wird ein Planning durchgeführt und nach dem Ende eines Sprints ein Retro. Da ich keine Ergebnisse an den Sprint-Enden präsentieren muss, wird jeweils kein Review stattfinden.

Daily Scrums werde ich jeden Tag als erste Tat durchführen. Die Erkenntnisse daraus werden im Arbeitsjournal festgehalten.

3.2 Anforderungsanalyse

In der Anforderungsanalyse werden Anforderungen zusammengestellt und die wichtigsten Komponenten beschrieben.

3.2.1 Analyse des Ist-Systems

3.2.1.1 Netzwerk

In der Suva setzt sich das Netzwerk aus einem Client- und Server-netz zusammen. Diese sind logisch voneinander getrennt und können dadurch ausschliesslich mittels einer Jump-Zone erreicht werden. Alle Systeme, welche der Endbenutzer für das tägliche Arbeiten benötigt, sind im Client-Netz. Dazu zählen Drucker und die Notebooks, die Clients. Hingegen im Server-Netz sind dann die Serversysteme untergebracht. Diese Netzwerk trennung wurde implementiert, damit die Server einen zusätzlichen Schutz vor Angriffen erhalten. Die Jump-Zone ist also das Bindeglied zwischen den beiden Netzen.

3.2.1.2 Physische Arbeitsstationen

Der Endbenutzer verwendet in der Suva normalerweise eine physische Arbeitsstation, genauer, ein Notebook. Seit 2020 haben wir in der Suva einen neuen Workplace. Mit ein paar Ausnahmen wird seit dieser Einführung grundsätzlich nur noch mit diesen Notebooks gearbeitet.

Eingeführt haben wir das HP EliteBook x360 1040 G7:

Prozessor (CPU)	Intel Core i7-10810U CPU @ 1.10GHz 1.61GHz
Arbeitsspeicher (RAM)	16.0 GB
Hard Disk (Speicher)	512 GB NVMe SSD
Betriebssystem (OS)	Windows 10 Enterprise, Version 19044, 64 Bit
Endpoint Security	<u>Trellix</u>
Diskverschlüsselung	<u>BitLocker</u>

3.2.1.3 Virtuelle Arbeitsstationen

Zusätzlich zu den Notebooks gibt es jedoch auch virtuelle Desktops, VDIs. Das ist dann entweder eine persistent VDI oder eine JumpVDI. Die JumpVDI wird für die Verwaltung der Server verwendet und kann von IT-Mitarbeitern bestellt werden. Durch diese JumpVDI kann man nun also durch die Jump-Zone vom Client-Netz ins Server-Netz «hüpfen». Die persistent VDI hingegen dient quasi als einen zweiten Desktop/ein Zweitarbeitsgerät.

3.2.1.4 Serverumgebung

In der Suva werden hauptsächlich Windows Server 2019 eingesetzt, welche so gut wie nie physisch bereitgestellt werden. Alle Windows Server werden durch CrowdStrike Falcon optimal vor Viren geschützt. In der Suva werden auch Linux-Server eingesetzt. Diese sind jedoch nicht Teil dieser Arbeit.

Wenn man sich auf einen Windows Server verbinden möchte, muss man einen privilegierten Admin Account besitzen. Somit wird verhindert, dass unautorisierte Nutzer auf den Server gelangen. Man verbündet sich also mittels MFA auf eine JumpVDI. Von da aus geht es, mit Admin-Account, weiter über RDP auf den Server selbst. Auf dem Server ist kein Internetzugriff möglich.

3.2.1.5 Applikationen

Jegliche Applikationen werden nach heutigem Stand durch die Softwarelösung Matrix42 auf die Notebooks verteilt. Wenn eine Person eine spezielle Applikation benötigt, welche nur wenige benötigen, wird eine Handinstallation von einem IT-Techniker getätig. Der Identity Manager ist hierbei von beidem ausgenommen.

3.2.1.6 Identity & Access Management

Aktuell wird die Version 8.2.1 des Identity Managers produktiv verwendet. Mit dem Identity Manager von One Identity werden zurzeit alle Identitäten und Zugriffsberechtigungen verwaltet.

Eine zusätzliche Testumgebung nach Hersteller-Standard ist auf derselben Version vorhanden.

3.2.2 Soll-Systembeschreibung

Nach dem nun die Erfassung des Ist-Zustandes abgeschlossen ist, können Anforderungen aus den gewonnenen Daten festgelegt werden. Die Soll-Systembeschreibung basiert auf den Daten, welche in den Vorarbeiten beschafft wurden. Dabei wurde bereits abgeklärt, welche Anforderungen das IAM-Team definiert.

3.2.2.1 Zielkatalog

In diesem Zielkatalog werden die Ziele nach Muss- und Kann-Zielen bewertet. Die Muss-Ziele müssen im Detailkonzept detailliert beschrieben werden. Diese sind natürlich auch umzusetzen. Die Kann-Kriterien hingegen müssen nicht zwingend umgesetzt werden, sondern bieten lediglich die Option Erweiterungen durchzuführen, falls es die Zeit zulässt.

Muss-Kriterien sind meist aus der Aufgabenstellung oder der Definition von Sicherheit entstanden. Kann-Kriterien aber, entstanden aus Eigenüberlegungen und Gedanken.

Die unten zu sehende Tabelle stellt den eigentlichen Zielkatalog dar:

ID	Muss/Kann	Bezeichnung
1	Muss	Microsoft .NET 4.8 installieren
2	Muss	Identity Manager 9.1 installieren & konfigurieren
3	Muss	Alle aktiven Mitarbeiter importieren
4	Muss	LDAP Verzeichnis anschliessen
5	Muss	Identity Lifecycle implementieren
6	Muss	Benutzeranleitung verfassen
7	Muss	Big Picture der Systemarchitektur erstellen
8	Muss	Suva-Standards einhalten
9	Kann	Webshop Frontend installieren
10	Kann	Zusätzlicher Job-Service konfigurieren

Abbildung 15: Zielkatalog (Dätwyler, 2023)

3.2.2.1.1 (1) Microsoft .NET 4.8 installieren

Muss: Das Software-Framework «Microsoft .NET» in der Version 4.8 ist für den zu installierenden Identity Manager in der Version 9.1 eine Minimalanforderung. Dies gilt natürlich lediglich für Windows Betriebssysteme, weshalb es bei dieser Arbeit zum Zug kommen muss.

3.2.2.1.2 (2) Identity Manager 9.1 installieren & konfigurieren

Muss: Mit unter ein Hauptbestandteil dieser Arbeit besteht darin, den Identity Manager in der Version 9.1 zu installieren und konfigurieren. Zudem bietet es die Grundlage für die weiteren zu erreichenden Ziele.

3.2.2.1.3 (3) Alle aktiven Mitarbeiter importieren

Muss: Es sollen alle in der produktiven Umgebung aktiven Mitarbeiter ins vorhandene System importiert werden. Exportiert werden, müssen alle für den Identity Lifecycle notwendigen Felder.

3.2.2.1.4 (4) LDAP Verzeichnis anschliessen

Muss: Damit der Identity Lifecycle ausgiebig getestet werden kann, soll ein bereits vorhandenes LDAP Verzeichnis am Identity Manager angeschlossen werden.

3.2.2.1.5 (5) Identity Lifecycle implementieren

Muss: Ein weiterer Hauptbestandteil dieser Arbeit ist es, den Identity Lifecycle zu implementieren.

3.2.2.1.6 (6) Benutzeranleitung verfassen

Muss: Während der Identity Manager installiert und konfiguriert wird (wie auch wenn der Identity Lifecycle implementiert wird) muss dazu eine Benutzeranleitung erstellt werden. Dies soll dann eine Schritt-für-Schritt-Anleitung ergeben, in welcher es möglichst kein Interpretationsspielraum gibt.

3.2.2.1.7 (7) Big Picture der Systemarchitektur erstellen

Muss: Ein Big Picture der Systemarchitektur soll gezeichnet und dokumentiert werden.

3.2.2.1.8 (8) Suva-Standards einhalten

Muss: Während der Umsetzung müssen die Suva-Standards eingehalten werden. Darunter gehören Namensgebung, Security Richtlinien für LDAP Konten sowie die identische Konfiguration des Systems (bspw. die Configuration Parameter).

3.2.2.1.9 (9) Webshop Frontend installieren

Kann: Wenn es die Zeit erlaubt, gäbe es noch die Möglichkeit das Web-GUI, das Webshop Frontend, zu installieren. Über dieses Portal können Endbenutzer für sich oder Unterstellte verschiedene Berechtigungen ab-/bestellen.

3.2.2.1.10 (10) Zusätzlicher Job-Service konfigurieren

Kann: Als weiteres optionales Ziel habe ich noch aufgeschrieben, dass ich einen zusätzlichen Job-Service konfigurieren könnte.

3.3 Detailkonzept

Im Detailkonzept wird die konzeptionelle Umsetzung meiner Arbeit beschrieben. Es werden keine Modelle eingesetzt, da keine Modelle zur Anwendung vorhanden sind.

3.3.1 Systemlandschaft – Internes IAM

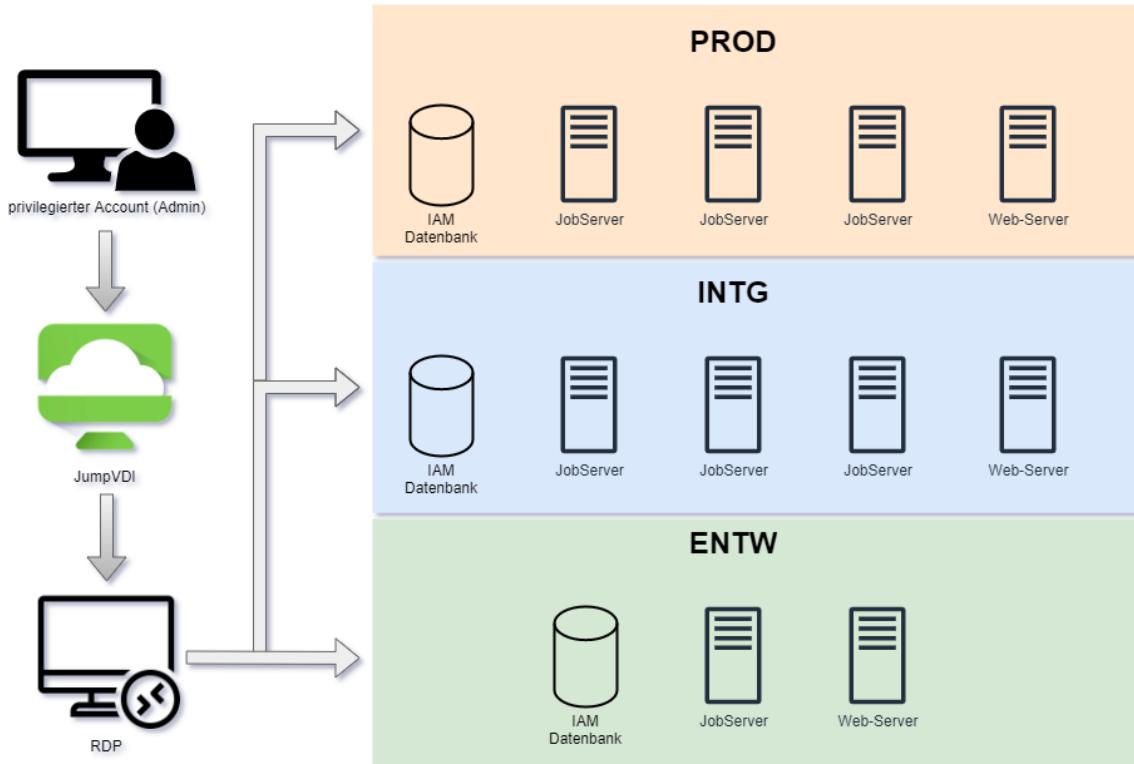


Abbildung 16: Systemlandschaft – Internes IAM (Dätwyler, 2023)

Im oben abgebildeten Big Picture kann man die Systemlandschaft des internen IAMs der Suva entnehmen. Ich habe, um es möglichst simpel und allgemein darzustellen, hierbei keine Server-Namen verwendet oder Funktionen erwähnt. Zudem möchte das IAM Team in der Suva nicht, dass interne Server-Namen nach aussen gelangen. Zu sehen ist das Prinzip des Verbindens auf Windows Server, wie wir es in der Suva handhaben. Erklärt habe ich dies bereits im Kapitel «3.2.1.4 Serverumgebung». Von der JumpVDI aus, kann man sich nun auf die Server der Stufe ENTW, INTG oder PROD verbinden. In der Suva gibt es nebst diesen drei Stufen noch andere Stufen, auf welchen jedoch kein IAM-System läuft.

Die INTG ist identisch zur PROD, wie man in der Abbildung oben erkennen kann. Die ENTW hingegen ist nicht identisch zu den anderen beiden Stufen. Der Sinn und Zweck hinter den Stufen ist: Man entwickelt und testet in der ENTW und transportiert diese Änderung mittels Transport-File in die INTG und kann somit testen, ob der Transport funktioniert oder nicht. Wenn der Transport funktioniert, kann eine weitere Transportierung der Änderungen, nun von INTG in die PROD, durchgeführt werden.

3.3.1.1 Schnittstellen zur Aussenwelt

In dieser PA werde ich mich ausschliesslich auf der Stufe ENTW aufhalten, weswegen ich kein System ausserhalb dieser Segmentierungsstufen ansprechen werden. Es wird somit keine Schnittstellen zu anderen IAM Systemen geben. Die einzigen Schnittstellen sind die Zielsysteme LDAP und CSV sowie die Datenbank meiner IAM-Umgebung.

Andere Teilsysteme mit Abhängigkeiten sind nicht vorhanden.

3.3.2 Failover-Szenarien

3.3.2.1 Netzwerk-Ausfall in der Suva

In der Suva wurde eine redundante Netzwerkinfrastruktur aufgebaut, sprich, wenn eine Netzwerk-Seite ausfallen würde, könnte eine, von der ersten Seite unabhängige, Netzwerkinfrastruktur, die Aufgabe der ausgefallenen Seite übernehmen.

3.3.2.2 Rechenzentrums-Ausfall in der Suva

Es sind in der Suva zwei Rechenzentren redundant im Betrieb, welche geografisch voneinander getrennt sind. Das eine kann dabei jeweils bei einem Ausfall durch äussere Einwirkung das andere RZ übernehmen.

3.3.3 Benutzeranleitung

Zur Installation und Konfiguration des Identity Managers, soll eine Schritt-für-Schritt-Benutzeranleitung erstellt werden. In derselben Benutzeranleitung werde ich auch die Implementation des Identity Lifecycle festhalten. Diese Anleitung wird von mir so präzise kreiert, dass die Anweisungen nicht missinterpretiert werden können und sie keine Fragen offenlassen. Meine persönlichen Fehltritte, wenn welche vorkommen, werden transparent dokumentiert, damit ein potenzieller Leser nicht denselben Fehler begeht. Zu Beginn der Benutzeranleitung gebe ich eine Übersicht der Voraussetzungen und der Schritte, damit der Leser besser verstehen kann, was auf ihn zukommt.

3.3.4 Identity Lifecycle

Um die Aufgabe, einen Identity Lifecycle zu implementieren, vereinfacht darzustellen, habe ich das im Kapitel «2.2.3 Identity Lifecycle» beschriebene Konzept unten grafisch dargestellt. Zu sehen ist, wie der Identity Lifecycle in dieser Arbeit funktionieren soll. (Floatchart → Anhang)

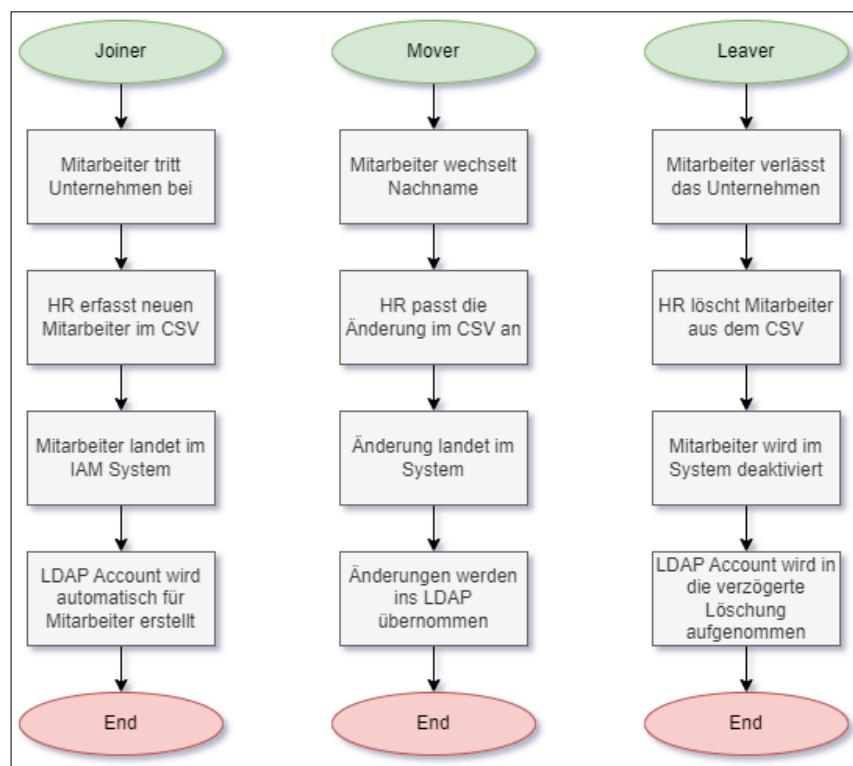


Abbildung 17: Identity Lifecycle (Dätwyler, 2023)

3.3.5 Lösungsvarianten

Für die Implementation des Identity Lifecycles gibt es verschiedene Implementationsvarianten.

Die Einflussgrössen dieser beschränken sich auf das von mir zu installierende IAM System. Die Auswirkungen einer Implementation nehmen Folge auf die Erstellung und Löschung von Zielsystemkonten wie LDAP Accounts und können Identitäten der IAM Datenbank deaktivieren.

3.3.5.1 Manuelle Zuteilung

Hierbei erstellt man im **Manager** manuell einen LDAP Account pro Identität. Dies weist natürlich keinen Automatisierungsgrad auf und ist keinesfalls effizient. Wenn man lediglich ein paar vereinzelte Accounts erstellen muss, ist diese Variante aber durchaus eine Option. Diese Variante wird in dieser PA von mir **nicht verwendet**.

3.3.5.2 Account Definition

Im **Manager** unter «LDAP» kann man «Account Definitions» erstellen. Die erstellte Account Definition kann dann wiederum einer Identität angehängt werden und es wird automatisch ein Account für diese erstellt. Da die Prozessautomatisierung in diesem Fall nicht komplett ausgeschöpft wird, werde ich diese Lösungsvariante **nicht verwenden**.

3.3.5.3 Account Definition mit Department

Eine Account Definition kann auch gemeinsam mit einem Department implementiert werden. Nach dem man die Account Definition hat, erstellt man noch ein Department, welchem man eine «Account Definition» zuweist. Bei jedem Mitarbeiter, der nun dieser Organisation hinzugefügt wird, wird die Account Definition angewandt. Diese Variante weist bereits einen hohen Automatisierungsgrad auf, ist jedoch nicht Suva-Standard, weshalb ich diese Lösungsvariante **nicht verwenden** werde.

3.3.5.4 Account Definition mit Geschäftsrolle

Eine Account Definition kann auch zusätzlich in Kombination mit einer Geschäftsrolle implementiert werden. Man erstellt also nach dem man die Account Definition hat noch eine Geschäftsrolle, wobei man als Erstes eine Role Class mit der Zuweisung «Account Definition» erstellt. Danach kreiert man noch eine «dynamische Rolle» aus der Geschäftsrolle. Das heisst, man kann eine SQL-Where-Klausel mitgeben, welche bspw. auf alle aktiven Mitarbeiter filtert. Somit wird die Geschäftsrolle bei jeder Identität angehängt, bei der das SQL-Query zutrifft und somit die Account Definition angewandt. Damit ich den Automatisierungsgrad am höchsten halten kann und gleichzeitig den Suva-Standard befolgen kann, werde ich in dieser PA diese Variante **verwenden**.

3.3.5.5 Meine Variante

Die Implementationsvariante «Account Definition mit Geschäftsrolle» ist in meinen Augen am besten für eine Prozessautomatisierung geeignet, weswegen ich diese in meiner Arbeit verwende. Zudem wird in der Suva auch mit dieser Variante gearbeitet.

Um die Lösung vereinfacht darzustellen, findet sich unten eine grafische Darstellung des Implementationsprozesses. Dieser dient als Handlungsplan. (Flowchart → Anhang)

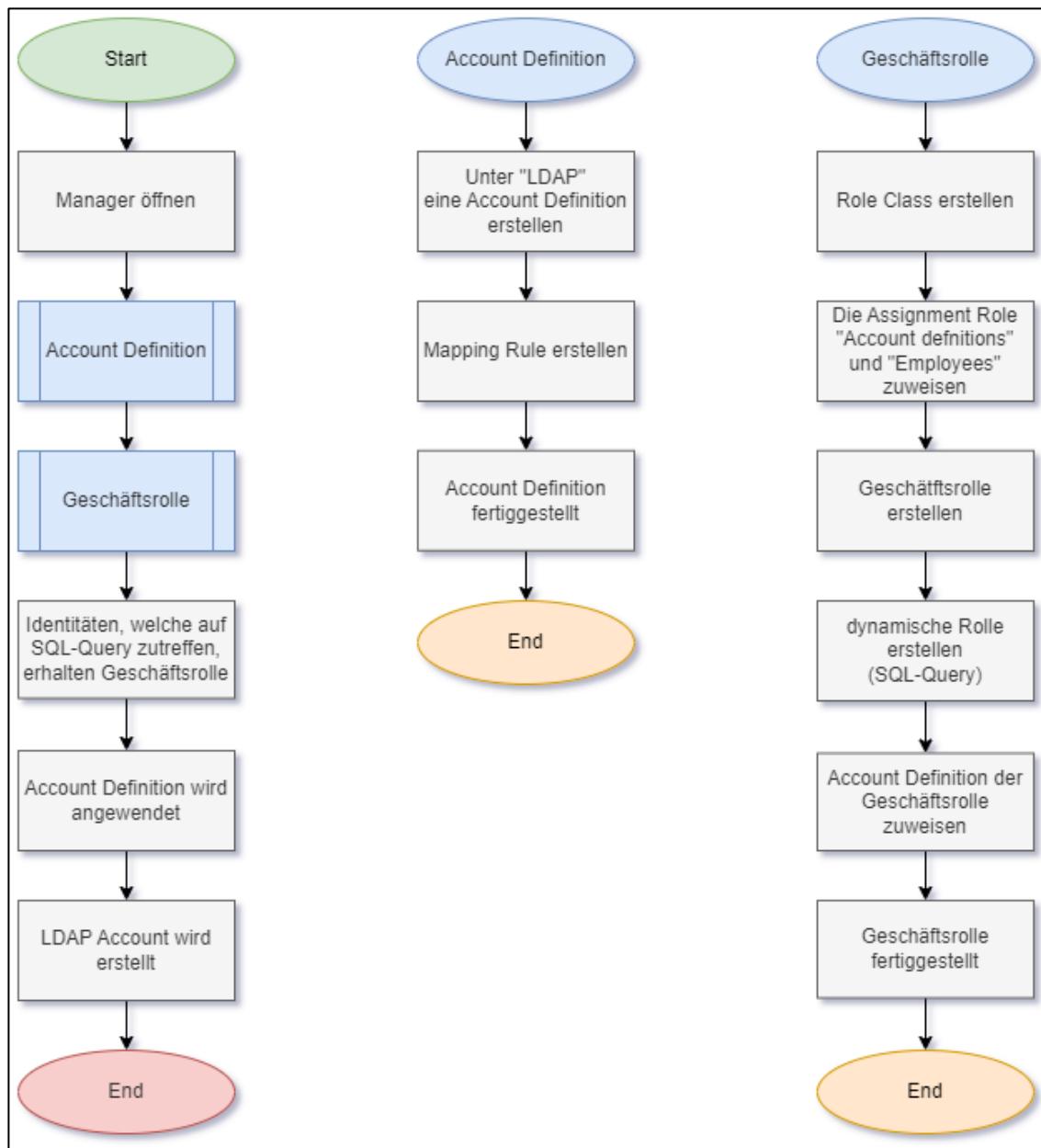


Abbildung 18: Implementationsprozess (Dätwyler, 2023)

3.4 Umsetzung

3.4.1 Labor-Aufbau

3.4.1.1 Installation und Konfiguration nach Suva-Standard

Installiert wurde die Version 9.1 des Identity Managers von [One Identity](#). Zur Verfügung stand mir dafür eine interne Installationsanleitung der Version 7.0.2 (Vogt, 2016) sowie der Version 7.1 (Vogt, 2016). Des Weiteren fanden sich noch die sämtlichen Security Richtlinien (Stadelmann, 2023) inkl. DB-Verschlüsselung (Vogt, 2022) in unserem internen Wiki. Damit ich die Konfiguration nach Suva-Standard machen konnte, benötigte ich noch einen Vergleich der Configuration Parameters, welchen ich ebenfalls im internen Wiki fand (Dätwyler, 2022). Die Release Notes zur Version 9.1 (One Identity, 2023) hatte ich bereits im Vorhinein studiert.

Auf welchem System die Installation stattfand, wurde bereits im Kapitel «3.3.1 Systemlandschaft – Internes IAM» festgehalten.

3.4.1.1.1 Installation

Ich habe mich als Erstes über die im Kapitel «3.2.1.4 Serverumgebung» beschriebene Methode auf unseren Server begeben, auf welchem es geplant war, die Installation auszuführen.

Das Erste, was ich auf dem Server tat, war, dass ich [Microsoft .NET](#) in der Version 4.8 installiert habe. Dies hat auch ohne weitere Probleme so funktioniert. Nach einem Neustart konnte ich auch schon mit der eigentlichen Installation, die des Identity Managers, beginnen.

Zuerst musste ich mich durch ein Setup klicken, worin ich bspw. auswählen musste, welche Version ich verwenden möchte oder wo das Installationsverzeichnis liegen soll. Ich konnte dann noch meine gewünschten Module sowie die Machine Roles wählen. Nachdem ich den Standard Job-Service nach Suva-Standard anpassen konnte, war das Setup auch bereits fertig und ich konnte mit der Installation der IAM-Datenbank beginnen.

Ich verband mich also mit der beim DBA zuvor bestellten Datenbank mittels unserem SQL-Admin-User. Nach ein paar weiteren Überprüfungen von unter anderem den zuvor gewählten Modulen, wurde die Datenbank auch schon installiert. Jetzt konnte ich noch den Suva-Standard-User anlegen, welche Berechtigungen analog zum «viadmin» besitzen sollte. Mit der Verschlüsselung der DB konnte ich dann die Installation erfolgreich beenden.

3.4.1.1.2 Konfiguration

Nun war es an der Zeit, den Job-Service zu konfigurieren. Im **Designer** musste ich ein paar Benennungsanpassungen durchführen sowie die benötigten Server-Funktionen und Machine Roles für den Job-Server aktivieren. Im **JobServiceConfigurator** musste ich verschiedenste Attribute anpassen, damit ich den Suva-Standard einhalten konnte.

Nachdem der Job-Service nun konfiguriert wurde, mache ich mich an die Config. Parameter. Hierbei ging es darum, alle Anpassungen, welche nach Suva-Standard durchgeführt wurden, in dieser Installation ebenfalls so umzusetzen.

Weiter kontrollierte ich im **Designer**, ob die Schedules aktiviert sind, was sie waren, und überprüfte die Security Richtlinien.

3.4.1.2 Mitarbeiter Export / Import

Nach der Konfiguration habe ich mich an den Export bzw. Import der aktuell aktiven Mitarbeiter gemacht. Insgesamt musste ich 5'455 Personen ex-/importieren.

3.4.1.2.1 CSV Anbindung

Zu Beginn startete ich den **Object Browser** auf der Stufe PROD. Daraus las ich dann alle aktiven, reellen Personen in eine CSV-Datei. Ich benutzte dazu folgendes SQL-Query:

```
SELECT CentralAccount, FirstName, LastName, EntryDate, ExitDate
FROM Person
WHERE IdentityType = 'Primary' AND IsInactive = 'False'
```

Attribut	Grund
CentralAccount	Identifikationsnummer, um die Identitäten voneinander zu unterscheiden
FirstName	Pflichtfeld im System und zur Darstellung
LastName	Pflichtfeld im System und zur Darstellung
EntryDate	Für den Identity Lifecycle-Test
ExitDate	Für den Identity Lifecycle-Test

Abbildung 19: Export – Attribut/Grund (Dätwyler, 2023)

Filter	Nutzen
IdentityType = Primary	Es werden nur reelle Personen angezeigt
IsInactive = False	Alle deaktivierten Personen werden nicht angezeigt

Abbildung 20: Export – Filter/Nutzen (Dätwyler, 2023)

Ich kopierte dieses CSV auf den Server, auf welchem sich meine IAM-Installation befindet. Im IAM-System öffnete ich dann den **Synchronization Editor**. Ich hängte mein CSV an und führte darauf, sowie auf dem Identity Manager selbst, ein Schema Update durch.

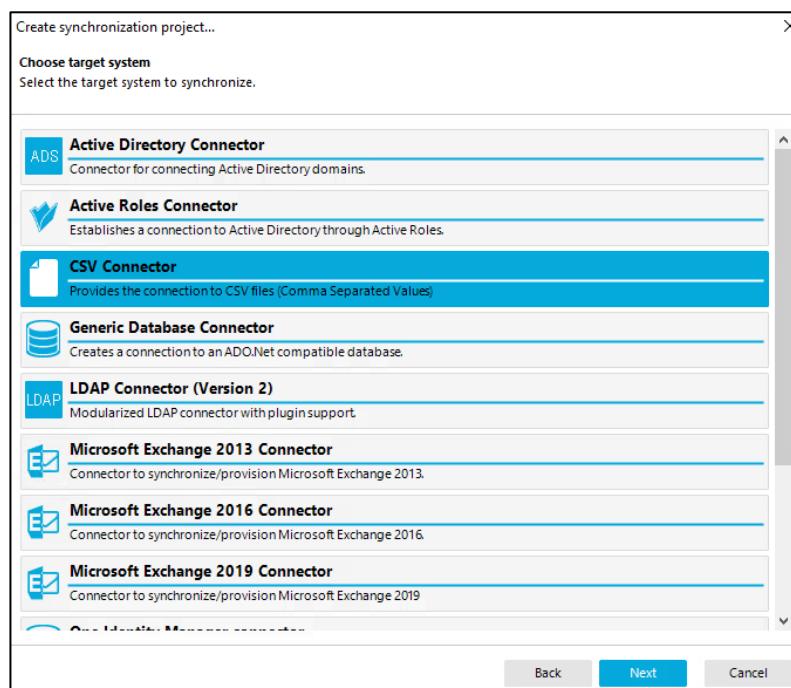


Abbildung 21: CSV anhängen (Dätwyler, 2023)

Damit die Synchronisation überhaupt funktionieren konnte, muss ich noch ein Base object hinzufügen. Bis ich zu dieser Realisation gekommen bin, brauchte ich jedoch ein paar Minuten.

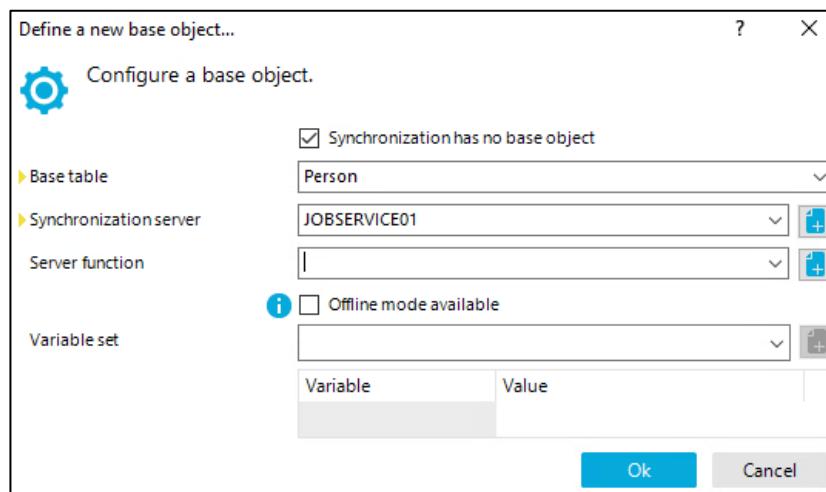


Abbildung 22: Base object erstellen (Dätwyler, 2023)

Danach musste ich noch ein Mapping erstellen, durch welches die Daten des Zielsystems mit den Daten der IAM-Datenbank abgeglichen werden.

Abbildung 23: CSV mit Identity Manager mappen (Dätwyler, 2023)

Ich musste dann noch in einem Workflow angeben, welche Synchronisations-Methoden (Insert, Delete, Update...) verwendet werden sollen.

Abbildung 24: Synchronization Workflow (Dätwyler, 2023)

Um nun eine Simulation starten zu können, musste ich erst noch eine Startup-Config. einrichten, mit welcher ich diese, und danach auch die eigentliche Synchronisation, starten konnte.

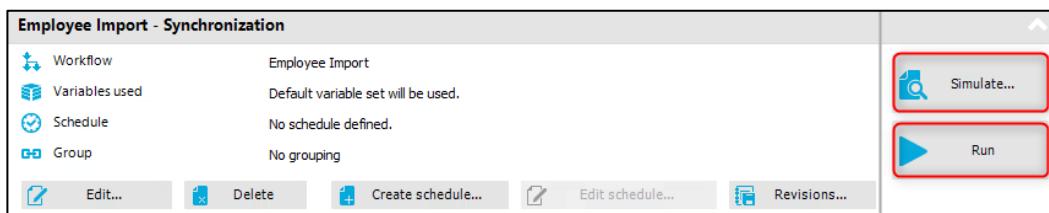


Abbildung 25: Startup-Config. (Dätwyler, 2023)

3.4.1.2.2 Nachweis

Nach einer erfolgreichen Simulation konnte ich dann das Projekt aktivieren und die Synchronisation starten, was ohne Probleme funktionierte.

Eingelesen habe ich somit 5'455 Mitarbeiter.

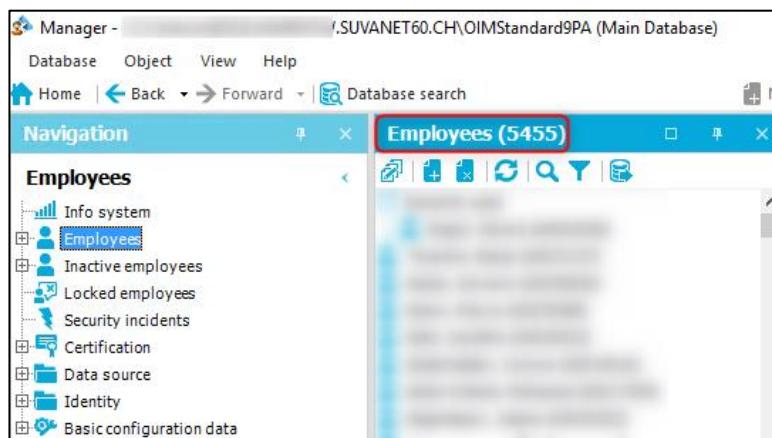


Abbildung 26: CSV-Import Nachweis (Dätwyler, 2023)

Der Nachweis des Imports wurde hierbei als Screenshot dar gegeben, da es mir aus Datenschutzgründen nicht möglich ist, das CSV offenzulegen.

3.4.1.3 LDAP Verzeichnis

Als Nächstes habe ich direkt schon das bereits vorhandene LDAP Verzeichnis angehängt. Da das Verfahren dazu im Prinzip dasselbe wie beim CSV ist, gehe ich hierbei nicht weiter darauf ein.

Eingelesen habe ich somit insgesamt 147 LDAP Accounts.

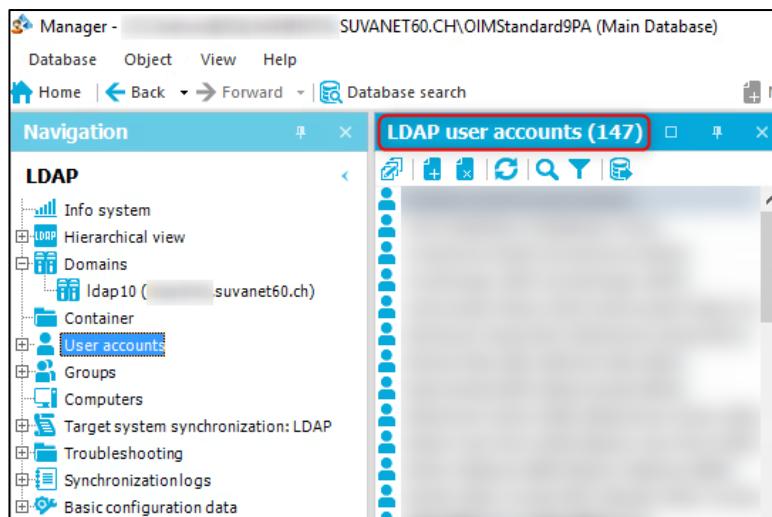


Abbildung 27: LDAP-Import Nachweis (Dätwyler, 2023)

3.4.2 Identity Lifecycle

Nun waren alle Mitarbeiter importiert, sowie auch alle vorhandenen LDAP Accounts. Jetzt ging es noch darum, den Identity Lifecycle zu implementieren.

3.4.2.1 Account Definition mit Geschäftsrolle implementieren

Im **Manager** erstellte ich als Erstes die Account Definition. Die reine Erstellung dieser bringt jedoch wahrlich wenig, weshalb zu dieser zusätzlich eine Mapping Rule erstellt werden musste. Dabei gibt man den Standort im LDAP Verzeichnis an, wo die neu zu erstellenden LDAP Accounts gespeichert werden sollen. Danach ist die Account Definition komplett fertiggestellt.

Jetzt musste ich noch eine Geschäftsrolle erstellen. Dazu erstellte ich zuerst eine Role Class, welcher ich die Role Assignments «Account Definition» und «Employees» hinzufügte. Danach kreierte ich die eigentliche Geschäftsrolle, welcher ich, nach Suva-Standard, den Namen «GR0000 | LDAP Account» gab. Ich erstellte, auf Basis dieser GR, eine dynamische Rolle. In dieser konnte ich dann eine SQL-Where-Klausel mitgeben, welches auf bestimmte Identitäten filtert. Somit kann man entscheiden, welche Personen/Identitäten diese GR bekommen sollen und damit für welche Identität ein LDAP Account erstellt werden soll.

Normalerweise hätte ich dafür folgende Abfrage verwendet:

```
CentralAccount LIKE 'A00%' AND IsInactive < 1
```

In diesem Fall habe ich jedoch direkt eine spezifische Identifikationsnummer einer bestimmten, noch fiktiven Identität angegeben, da sich meine Tests mit dieser, in den Tests noch zu erstellender, Identität abspielen werden.

```
CentralAccount = 'A0000000' AND IsInactive < 1
```

Jetzt musste ich lediglich noch die erstellte Account Definition der erstellten GR zuweisen.

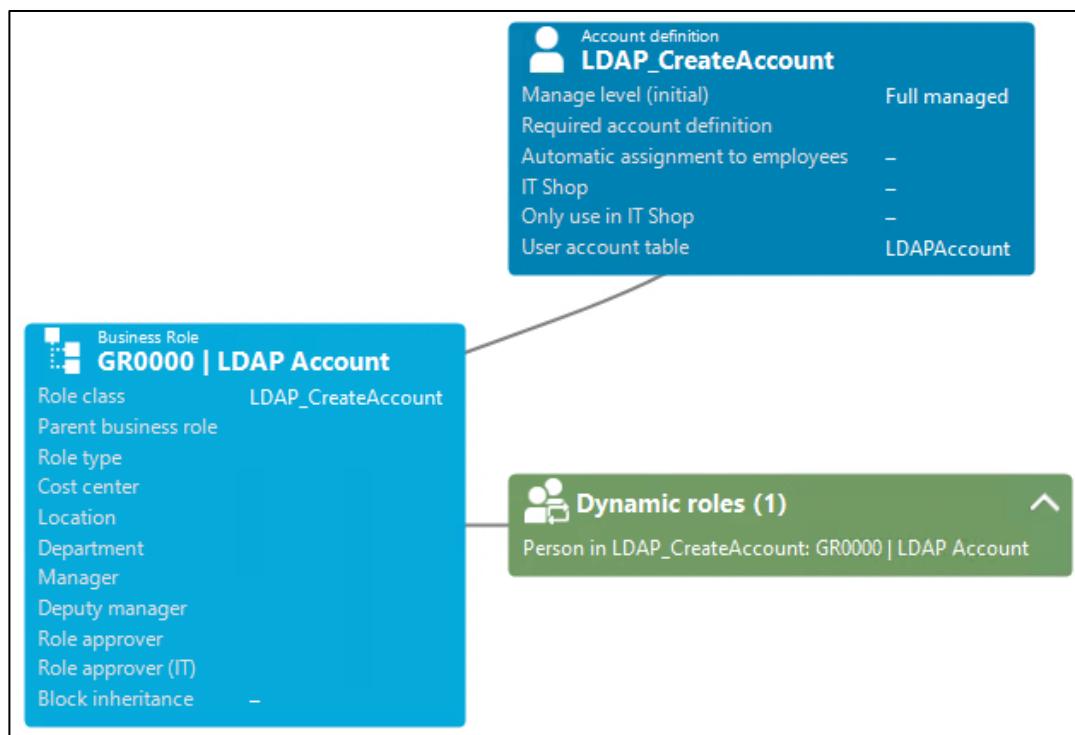


Abbildung 28: Account Definition mit Geschäftsrolle (Dätwyler, 2023)

3.4.3 Sicherheitsaspekte

3.4.3.1 Gefahren

Eine der grössten Gefahren in der IT-Security bildet sich aus dem Server-Zugriff von unautorisierten Nutzern. Wenn dieser Zugriff erfolgt, ist es umso wichtiger, dass Systeme wie das IAM strenge Security Richtlinien in Bezug auf hochprivilegierte Admin-User besitzt. Wenn ein Angreifer an einen IAM-Admin-User heran gelangt, kann der Angreifer mit diesem einen enorm hohen Schaden am System anrichten.

Angreifer könnten Viren verwenden, um an Daten von hochprivilegierten Usern zu gelangen, weshalb von Viren ein sehr hohes Sicherheitsrisiko ausgeht.

Eine Gefahr geht auch vom Thema Datendiebstahl aus. Angreifer könnten versuchen, vertrauliche Mitarbeiterdaten zu stehlen. Damit verbunden ist jedoch auch eine rechtliche Gefahr, denn ich bin in dieser PA ebenfalls dazu verpflichtet jegliche Personendaten zu schützen und nicht zu publizieren.

3.4.3.2 Lösungen

3.4.3.2.1 Server und Client

Auf dem Server werden nach dem Suva-Standard bereits entsprechende Sicherheitsvorkehrungen getroffen. Der Server kann nur mittels JumpVDI erreicht werden, auf welche sich nur Admins mit MFA verbinden können. Auf dem Server selbst ist kein Internetzugriff möglich und es ist, wie auch auf dem Client, mit welchem man sich auf diesen verbindet, ein optimaler Virenschutz installiert.

Das Ganze ist im Kapitel «3.2.1.4 Serverumgebung» sowie «3.2.1.2 Physische Arbeitsstationen» noch detaillierter beschrieben.

3.4.3.2.2 User/Group Accounts

Für mein IAM-System erstellte ich während der Installation einen benutzerdefinierten Admin-User, welcher dem IAM-Standard der Suva entspricht. Das Passwort des Admin-Users habe ich in unserem sicheren internen Passwortverwaltungstool abgelegt.

Im **Designer** kontrollierte ich dann, ob dieser IAM-Admin-User die gleichen Berechtigungen erhielt wie der «viadmin», was zutreffend war. Im gleichen Zug konnte ich auch direkt feststellen, dass kein anderer, wo möglich sogar passwortloser, IAM-User diese hoch privilegierten Berechtigungen besitzt.

Nun mussten die LDAP Accounts noch geschützt werden. Dafür konfigurierte ich die bis anhin eher mässig strenge Passwort-Richtlinie nach Suva-Standard (Stadelmann, 2023) neu.

3.4.3.2.3 Datenschutz

Um die Suva IT-Security-technisch zu schützen, habe ich jegliche Daten/Namen, welche ich als kritisch empfand, durch einen Blur zensiert – dasselbe gilt für jegliche Personendaten. Das jeweils Zensierte wurde nach interner Absprache entsprechend gewählt. Darunter fallen Admin-Accounts sowie die Admin-User des IAM-Systems oder von SQL. Zusätzlich zu den Accounts sind auch alle Server-Namen unkenntlich gemacht.

3.4.4 Systemarchitektur

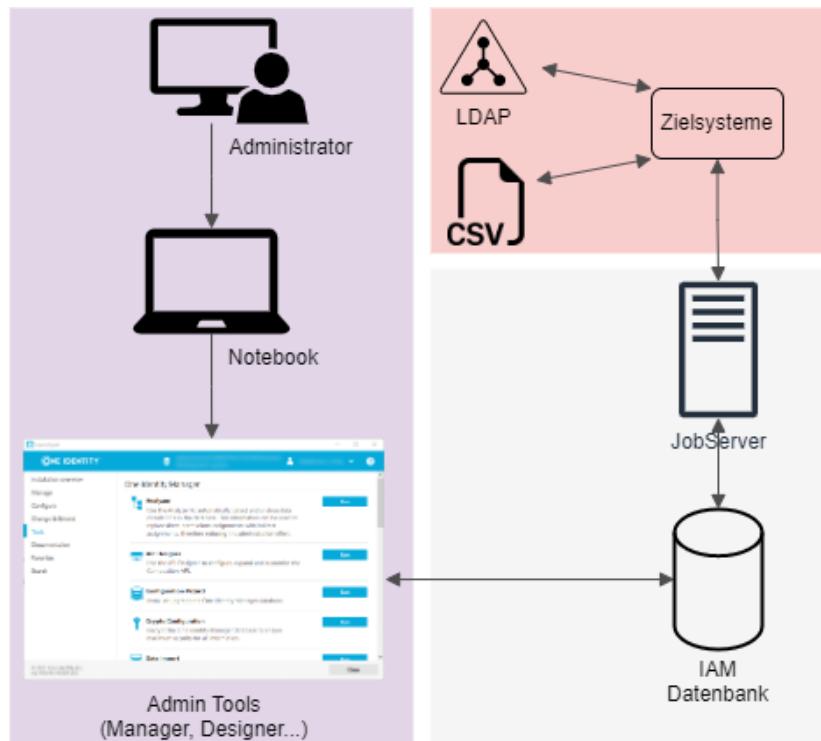


Abbildung 29: Systemarchitektur – 1IM Standard 9.1 PA (Dätwyler, 2023)

Abgebildet ist hier die Systemarchitektur vom von mir in dieser Arbeit aufgesetzten IAM-System. Das System trägt den Namen «1IM Standard 9.1 PA». Nach erfolgreicher Installation waren dann zwei Zielsysteme angeschlossen: Das LDAP und ein CSV, welche ich beide in dieser Arbeit verwende. Das Bindeglied zwischen den Zielsystemen und der IAM Datenbank stellt hierbei ein Job-Server dar.

Um das IAM verwalten zu können, benötigt man Zugriff auf die Admin-Tools. Diese wurden nach Suva-Standard auf dem Server installiert. Zusätzlich könnte jedoch auch ein IAM-Admin auf sein eigenes Notebook genau diese Admin-Tools installieren und somit das IAM-System vom eigenen Gerät aus verwalten.

Dies habe ich, wie man anhand der obigen Abbildung unschwer erkennen kann, ebenfalls so umgesetzt.

3.5 Testing

3.5.1 Testkonzept

In diesem Kapitel werden verschiedene Testfälle definiert. Das Ziel von diesen Testfällen ist es, das von mir aufgesetzte Labor sowie den von mir implementierten Identity Lifecycle auf Funktionalität zu überprüfen. Den groben Rahmen sollen dabei die im Kapitel «3.2.2.1 Zielkatalog» definierten Muss-Kriterien bilden.

3.5.1.1 Abgrenzung

Es werden in diesem Testing lediglich funktionale Tests durchgeführt, nämlich Systemtests, bei welchen das Labor an sich getestet wird, und Akzeptanztests, bei welchen die Anforderungen des Identity Lifecycles getestet werden.

Nicht getestet wird somit unter anderem die Performance, Zuverlässigkeit, Benutzbarkeit oder Übertragbarkeit des Labors, da dies nicht-funktionalen Tests sind. Durchgeführt werden diese nicht-funktionale Tests nicht, weil es sich in dieser praktischen Arbeit um eine nicht produktiv eingesetzte Testumgebung handelt, welche ein sich bisher bewährtes Tool, den Identity Manager, beinhaltet. Deswegen werden auch keine Sicherheitstests durchgeführt, obwohl dies in einer produktiven Umgebung essenziell wäre. Ebenso so wenig wird alles was im Kapitel «3.1.2 Abgrenzung» abgegrenzt wurde getestet, da dies nicht Teil dieser Arbeit ist.

3.5.1.2 Testziele

ID	Bezeichnung	Messgrösse
1	.NET Installation	Identity Manager kann installiert werden
2	IAM System Grundfunktionalität	Test-Identität kann angelegt werden
3	Schedules im Designer	Eingeplante Routine Jobs können gestartet werden und in den Log Files tauchen keine Fehler auf
4	Config. Parameter im Designer	Jobs tauchen in der Job History auf
5	Mitarbeiter Import mit CSV	Synch Projekt kann mit funktionstüchtigem Mapping erstellt und anschliessend mit dem IAM-System synchronisiert werden
6	Joiner	Importierte Identität erhält automatisch einen LDAP Account
7	Mover	Änderung im CSV wird bis zum LDAP Account übernommen
8	Leaver	Identität wird deaktiviert und LDAP Account in die verzögerte Löschung aufgenommen, nachdem das Austrittsdatum der Identität = Tagesdatum gesetzt wird

Abbildung 30: Testziele (Dätwyler, 2023)

3.5.1.3 Testsystem / Testumgebung

Alle Testfälle finden auf dem System, welches im Kapitel «3.4.4 Systemarchitektur» beschrieben wird, statt. Dieses System befindet sich auf Stufe ENTW, wie bereits im Kapitel «3.3.1 Systemlandschaft» beschrieben wurde. Somit werden alle Tests auf einem MS Windows Server 2016 durchgeführt. Die Verbindung auf diesen findet über unseren Client («3.2.1.2 Physische Arbeitsstationen») statt. Dies, indem wir uns auf eine JumpVDI verbinden (3.2.1.4 Serverumgebung).

3.5.2 Testfälle

3.5.2.1 Testfall 1: .NET Installation

ID	1
Bezeichnung	.NET Installation
Messgrösse	Identity Manager kann installiert werden
Testmethode	Systemtest manuell
Getestete Anforderung	Ziel 1
Testvoraussetzung	MS .NET 4.8 oder höher und MS Edge WebView2 müssen auf dem Server installiert sein.
Testmittel	<u>Microsoft .NET Framework 4.8</u> <u>Microsoft Edge WebView2</u> <u>Identity Manager 9.1 Setup</u>
Testablauf	Identity Manager Installation nach Suva-Standard. (Vogt, 2016)
Erwartetes Ergebnis	Installation wird erfolgreich durchgeführt werden.

Abbildung 31: Testfall 1 (Dätwyler, 2023)

3.5.2.1.1 Durchführung

Der Test bzw. die Installation wurde bereits im Kapitel «3.4.1.1.1 Installation» beschrieben, wie auch im Anhang, als Teil der Benutzeranleitung.

3.5.2.1.2 Ergebnis

Die Installation konnte erfolgreich durchgeführt werden und war anschliessend bereit für die Konfiguration und die weiteren praktischen Umsetzungen. Der Suva-Standard (Vogt, 2016) konnte durchgehend eingehalten werden, auch die DB Verschlüsselung (Vogt, 2022) verlief ohne Probleme. MS .NET wurde also korrekt installiert.

3.5.2.2 Testfall 2: IAM System Grundfunktionalität

ID	2
Bezeichnung	IAM System Grundfunktionalität
Messgrösse	Test-Identität kann angelegt werden
Testmethode	Systemtest manuell
Getestete Anforderung	Ziel 2
Testvoraussetzung	Identity Manager in der Version 9.1 ist installiert.
Testmittel	<u>Identity Manager 9.1</u>
Testablauf	Im Manager unter «Employees» erstelle ich eine Identität mit dem Namen «Test Identity».
Erwartetes Ergebnis	Es wird fehlerfrei möglich sein, denn die Installation wies keine grossen Probleme auf. Somit sollte nach der Durchführung eine Test-Identität auf meinem System existieren.

Abbildung 32: Testfall 2 (Dätwyler, 2023)

3.5.2.2.1 Durchführung

Ich öffne den **Manager** und begebe mich in die Kategorie «Employees». Dort kann ich eine neue Person/Identität anlegen. Dieser gebe ich dann einen Vor- und Nachnamen, ein Ein-/Austrittsdatum und eine Personalnummer.

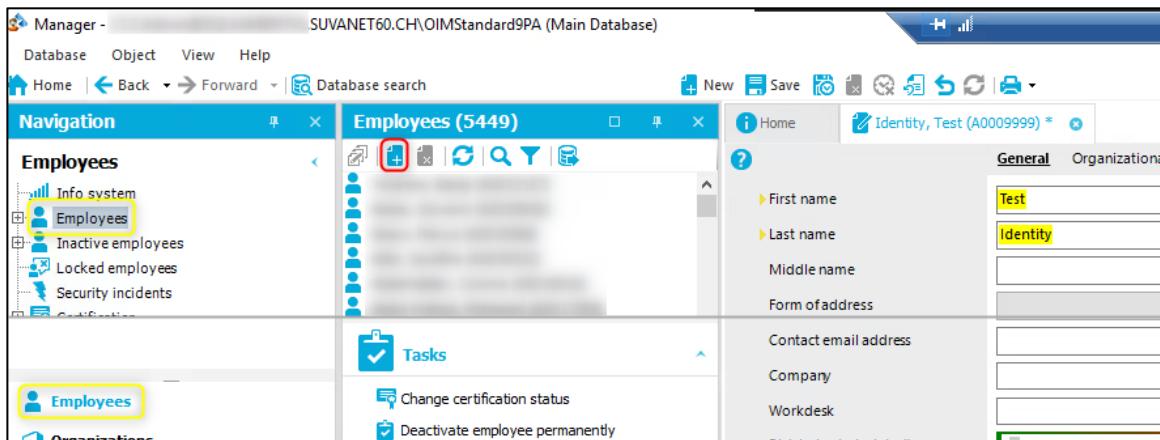


Abbildung 33: Testfall 2 – Test-Identität anlegen (Dätwyler, 2023)

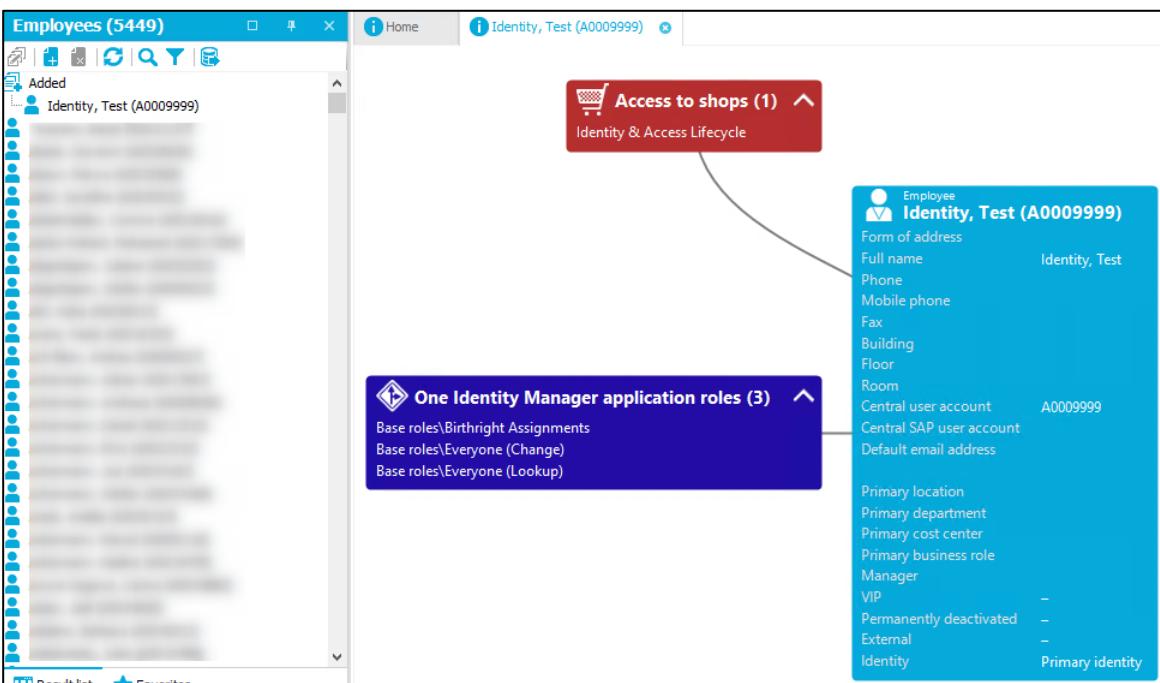


Abbildung 34: Testfall 2 – Test-Identität erfolgreich angelegt (Dätwyler, 2023)

3.5.2.2.2 Ergebnis

Das erwartete Ergebnis ist eingetroffen. Die Test-Identität konnte in kurzer Zeit problemlos angelegt werden, wie oben unschwer zu erkennen ist. Das bedeutet, dass die IAM-Grundfunktionalität bei meinem System zu funktionieren scheint.

3.5.2.3 Testfall 3: Schedules im Designer

ID	3
Bezeichnung	Schedules im Designer
Messgrösse	Eingeplante Routine Jobs können gestartet werden und in den Log Files tauchen keine Fehler auf
Testmethode	Systemtest manuell
Getestete Anforderung	Ziel 2
Testvoraussetzung	Identity Manager in der Version 9.1 ist installiert und konfiguriert.
Testmittel	<u>Identity Manager 9.1</u>
Testablauf	Im Designer starte ich die beiden Routine Jobs «Updates current UTC offsets for all time zones» und «Daily maintenance tasks» und kontrolliere danach die JobQueueInfo und die entsprechenden Logs.
Erwartetes Ergebnis	Die beiden Routine Jobs sollten problemlos ausgeführt werden können und daher in der JobQueueInfo ersichtlich sein.

Abbildung 35: Testfall 3 (Dätwyler, 2023)

3.5.2.3.1 Durchführung

Im **Designer** starte ich unter «Edit schedules» den Schedule «Daily maintenance tasks».

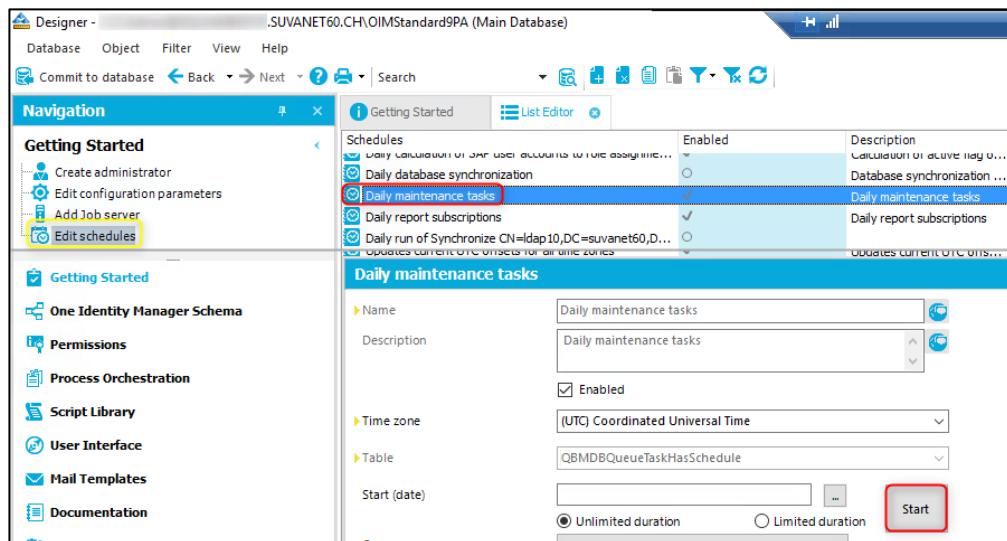


Abbildung 36: Testfall 3 – Schedule starten (Dätwyler, 2023)

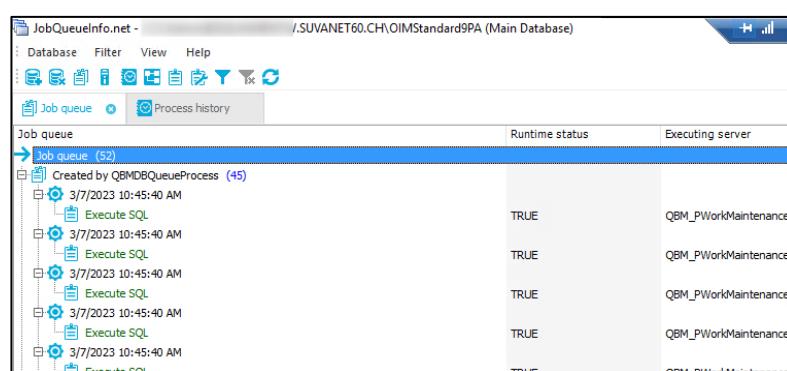


Abbildung 37: Testfall 3 – Jobs in der JobQueueInfo (Dätwyler, 2023)

Nachdem dieser durch ist, starte ich nun noch den «Updates current UTC offsets for all timezones»-Schedule.

Abbildung 38: Schedule starten (Dätwyler, 2023)

Abbildung 39: Jobs in der JobQueueInfo (Dätwyler, 2023)

3.5.2.3.2 Ergebnis

Die Routine Jobs konnten gestartet werden und in den Log Files konnte ich keine Fehler entdecken. Das Ergebnis fiel also wieder positiv aus. Die Logs dazu habe ich im Anhang dieses Dokumentes im Kapitel «Schedules – Log Files» angefügt, damit das Ganze auch nachvollzogen werden kann.

3.5.2.4 Testfall 4: Config. Parameter im Designer

ID	4
Bezeichnung	Config. Parameter im Designer
Messgrösse	Jobs tauchen in der Job History auf
Testmethode	Systemtest manuell
Getestete Anforderung	Ziel 2
Testvoraussetzung	Identity Manager in der Version 9.1 ist installiert und die Config. Parameter wurden nach Suva-Standard (Dätwyler, 2022) angepasst.
Testmittel	<u>Identity Manager 9.1</u>
Testablauf	Ich löse einen Schedule aus, und überprüfe, ob dieser in der Job History in der JobQueueInfo ersichtlich ist.
Erwartetes Ergebnis	Die Job History wurde von mir aktiviert, weshalb nach diesem Test das Ergebnis sein sollte, dass die Jobs vom ausgelösten Schedule gestartet werden sollen und nach Ablauf in der Job History ersichtlich sein werden.

Abbildung 40: Testfall 4 (Dätwyler, 2023)

3.5.2.4.1 Durchführung

Im Designer starte ich unter «Edit schedules» den Schedule «Daily maintenance tasks».

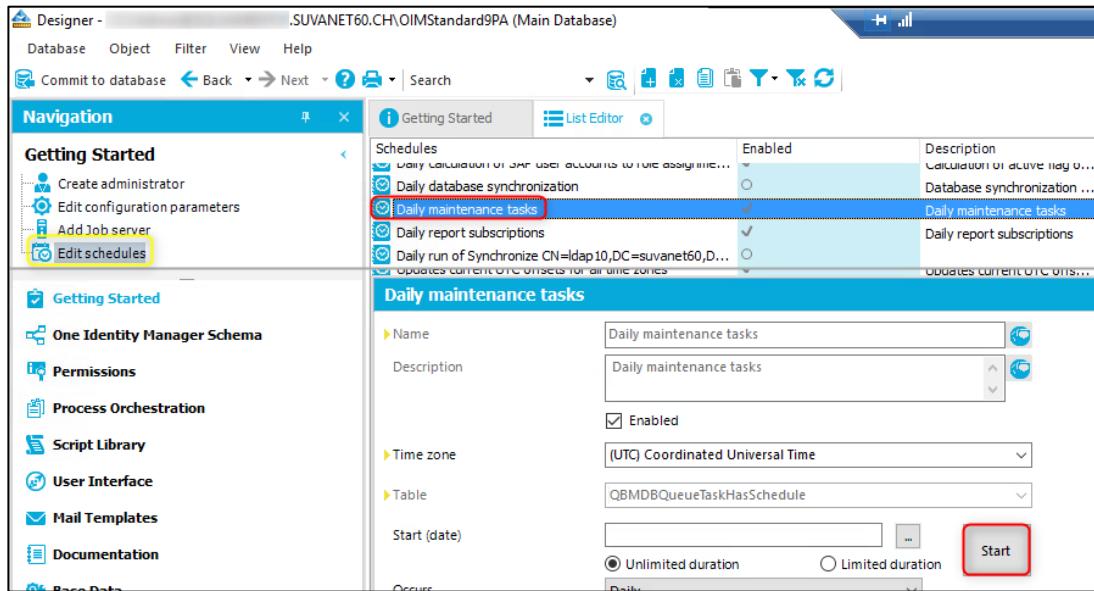


Abbildung 41: Testfall 4 – Schedule starten (Dätwyler, 2023)

In der **JobQueueInfo** unter «Process history» sind nun die bereits abgeschlossenen Jobs ersichtlich.

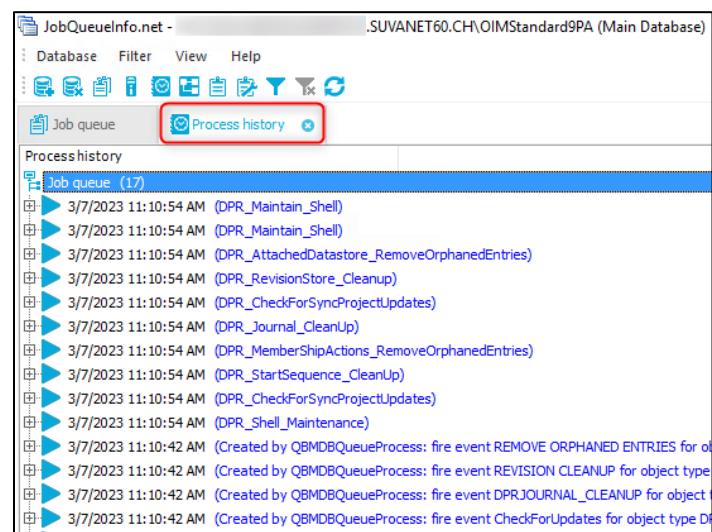


Abbildung 42: Testfall 4 – «Process history» in der JobQueueInfo (Dätwyler, 2023)

3.5.2.4.2 Ergebnis

Diesen Testfall konnte ich schnell abarbeiten, da, wie zu erwarten, alles reibungslos ablief, was man auch sehr schön an den obigen Screenshots entnehmen kann. Die Jobs tauchen also in der Job History, «Process history», auf.

3.5.2.5 Testfall 5: Mitarbeiter Import mit CSV

ID	5
Bezeichnung	Mitarbeiter Import mit CSV
Messgrösse	Synch Projekt kann mit funktionstüchtigem Mapping erstellt und anschliessend mit dem IAM-System synchronisiert werden
Testmethode	Systemtest manuell
Getestete Anforderung	Ziel 2 Ziel 3
Testvoraussetzung	Identity Manager in der Version 9.1 ist installiert und es wurde bereits ein Mitarbeiter Export aus der PROD in ein CSV durchgeführt.
Testmittel	<u>Identity Manager 9.1</u>
Testablauf	Im Synch Editor binde ich das exportierte CSV an und erstelle ein Mapping, sodass das CSV mit dem IAM-System synchronisiert werden kann.
Erwartetes Ergebnis	Der Testfall sollte reibungslos funktionieren, da ich keine Fehler bei der Installation erhielt. Es müssten nach dem Import etwas über 5'000 Identitäten im System sein.

Abbildung 43: Testfall 5 (Dätwyler, 2023)

3.5.2.5.1 Durchführung

Dieser Vorgang wurde bereits im Kapitel «3.4.1.2 Mitarbeiter Export / Import» ausführlich beschrieben.

3.5.2.5.2 Ergebnis

Das Test-Ergebnis ist, wie zu erwarten war, positiv ausgefallen. Es war nicht sehr anspruchsvoll, den Export auszuführen. Die richtige Reihenfolge bei der Anbindung des CSVs einzuhalten, war jedoch dafür ein bisschen schwieriger.

3.5.2.6 Testfall 6: Joiner

ID	6
Bezeichnung	Joiner
Messgrösse	Importierte Identität erhält automatisch einen LDAP Account
Testmethode	Systemtest/Akzeptanztest manuell
Getestete Anforderung	Ziel 4 Ziel 5
Testvoraussetzung	Identity Manager in der Version 9.1 ist installiert, das CSV und das LDAP Verzeichnis wurden angehängt und der Identity Lifecycle ist implementiert.
Testmittel	<u>Identity Manager 9.1</u>
Testablauf	Manuell eine neue Zeile (Identität → «Jane Doe») in der CSV-Datei ergänzen und dann mit dem IAM-Synchronisieren.
Erwartetes Ergebnis	Die Identität wird korrekt ins IAM-System aufgenommen und es wird ein entsprechender LDAP Account automatisch erstellt.

Abbildung 44: Testfall 6 (Dätwyler, 2023)

3.5.2.6.1 Durchführung

Ich öffne das CSV und ergänze es um eine Zeile.

A0000000;Jane;Doe;2017-04-20 00:00:00;2023-09-30 23:59:00

Abbildung 45: Testfall 6 – Neue CSV-Zeile (Dätwyler, 2023)

Im **Synchronization Editor** starte ich zuerst die Simulation und danach die eigentliche Synchronisation.

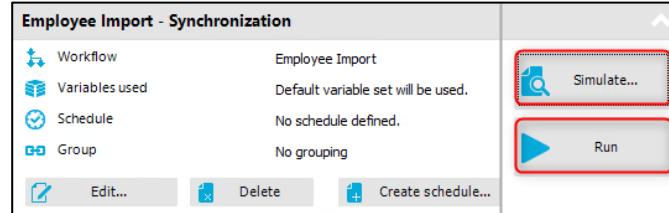


Abbildung 46: Testfall 6 – Synchronisation starten (Dätwyler, 2023)

Nach erfolgreicher Synchronisation ist «Jane Doe» importiert worden.

Normalerweise würde die Synchronisation über Nacht durchlaufen und meine erstellte dynamische Rolle würde neue Berechnungen durchführen. Somit wäre am nächsten Tag automatisch ein LDAP Account für die neue Identität erstellt. Da ich die Identität jedoch manuell am Tag hinzufüge, muss ich im **Manager** die Neuberechnung manuell starten.

Business Roles

- Info system
- LDAP_CreateAccount**
- Certification
- Troubleshooting
- Basic configuration data

GR0000 | LDAP Account

Tasks

- 1 Test condition
- 2 Start recalculation immediately

General

Role/organization: LDAP_CreateAccount: GR0000 | LDAP Account

Object class: Person

Dynamic role: LDAP_CreateAccount: GR0000 | LDAP Account

Calculation schedule: Dynamic roles check

Description: Creates an LDAP Account for an identity

Condition:

```
CentralAccount = 'A0000000' AND IsInactive < 1
--CentralAccount LIKE 'A00%' AND IsInactive < 1
```

Test result: Doe, Jane (A0000000)

1 - Object(s)

Abbildung 47: Testfall 6 – GR und Account Definition (Dätwyler, 2023)

Nachdem die Account Definition gezogen hat, ist nun ein LDAP Account erstellt worden.

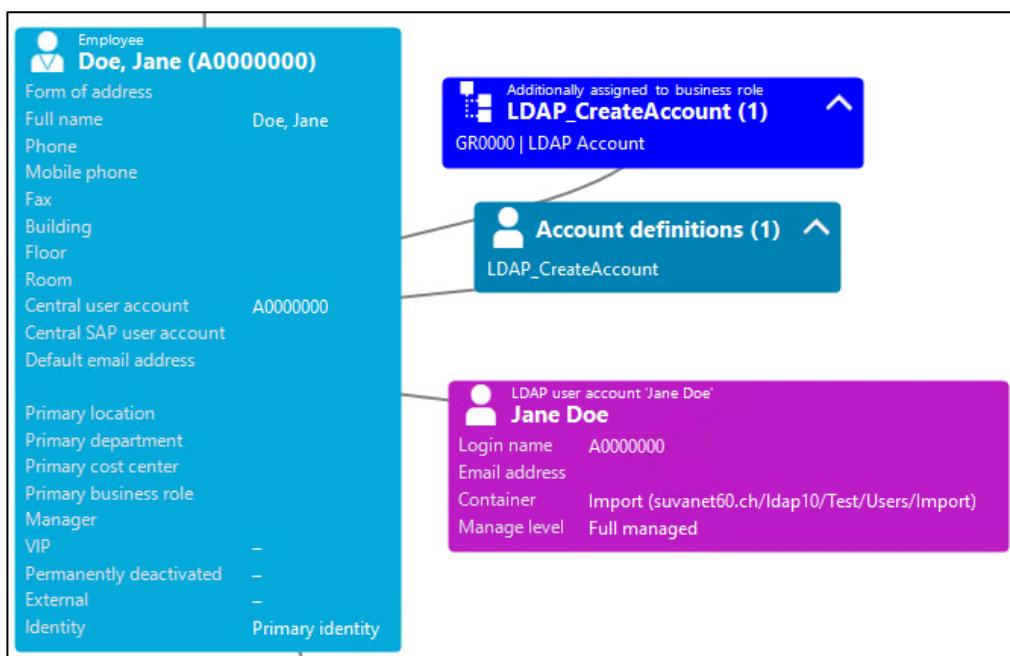


Abbildung 48: Testfall 6 – LDAP Account erstellt (Dätwyler, 2023)

3.5.2.6.2 Ergebnis

Das Ergebnis des Tests ist positiv ausgefallen. Aufgrund meiner kleinen Vorarbeit im Kapitel «3.4.2 Identity Lifecycle» konnte ich dies Test zügig abschliessen. Die Identität hat also einen LDAP Account erhalten.

3.5.2.7 Testfall 7: Mover

ID	7
Bezeichnung	Mover
Messgrösse	Änderung im CSV wird bis zum LDAP Account übernommen
Testmethode	Systemtest/Akzeptanztest manuell
Getestete Anforderung	Ziel 4 Ziel 5
Testvoraussetzung	Identity Manager in der Version 9.1 ist installiert, das CSV und das LDAP Verzeichnis wurden angehängt und der Identity Lifecycle ist implementiert.
Testmittel	<u>Identity Manager 9.1</u>
Testablauf	Den Nachnamen von «Jane Doe» im CSV zu «Jane Smith» ändern.
Erwartetes Ergebnis	Der LDAP Account wird dem CSV entsprechend angepasst – der Name wird von «Jane Doe» zu «Jane Smith» automatisch umbenannt.

Abbildung 49: Testfall 7 (Dätwyler, 2023)

3.5.2.7.1 Durchführung

Im CSV ändere ich den Nachnamen von «Doe» zu «Smith».

A0000000;Jane;Smith;2017-04-20 00:00:00;2023-09-30 23:59:00

Abbildung 50: Testfall 7 – Änderung im CSV (Dätwyler, 2023)

Im **Synchronization Editor** starte ich zuerst die Simulation und danach die eigentliche Synchronisation.

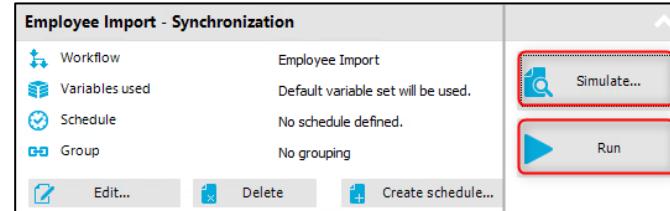


Abbildung 51: Testfall 7 – Synchronisation starten (Dätwyler, 2023)

Der Nachname wurde bei mir auf der Identität und auf dem Account nicht direkt gewechselt, weswegen ich diesen Schritt noch zusätzlich machen muss:

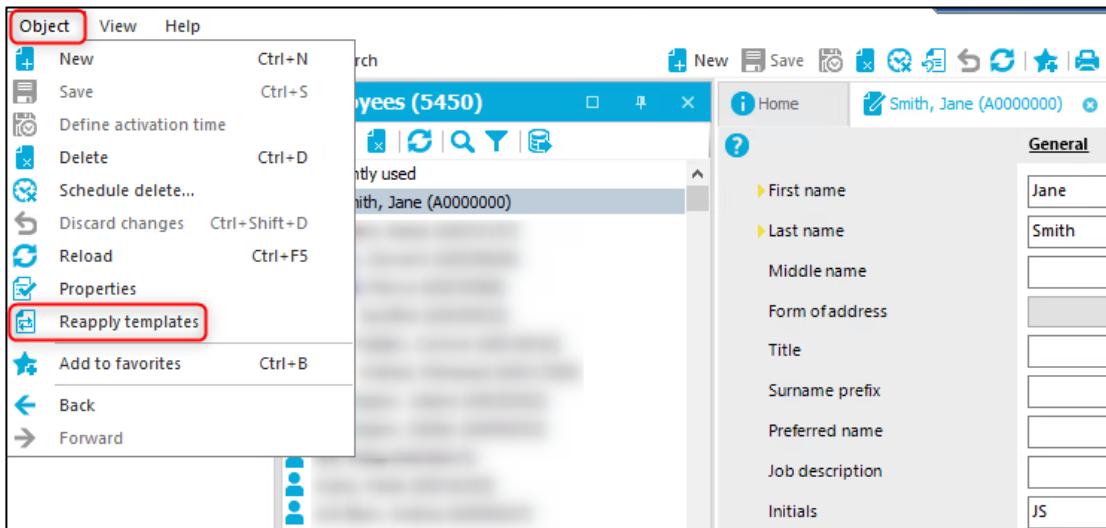


Abbildung 52: Testfall 7: Reapply templates [1] (Dätwyler, 2023)

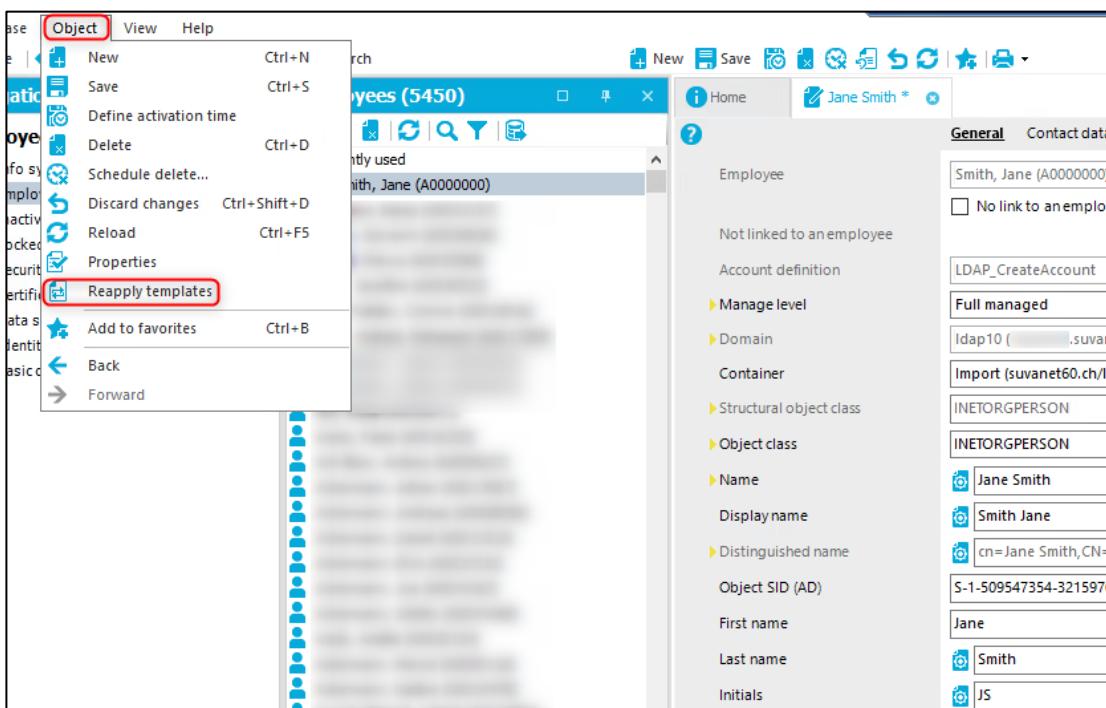


Abbildung 53: Testfall 7 – Reapply templates [2] (Dätwyler, 2023)

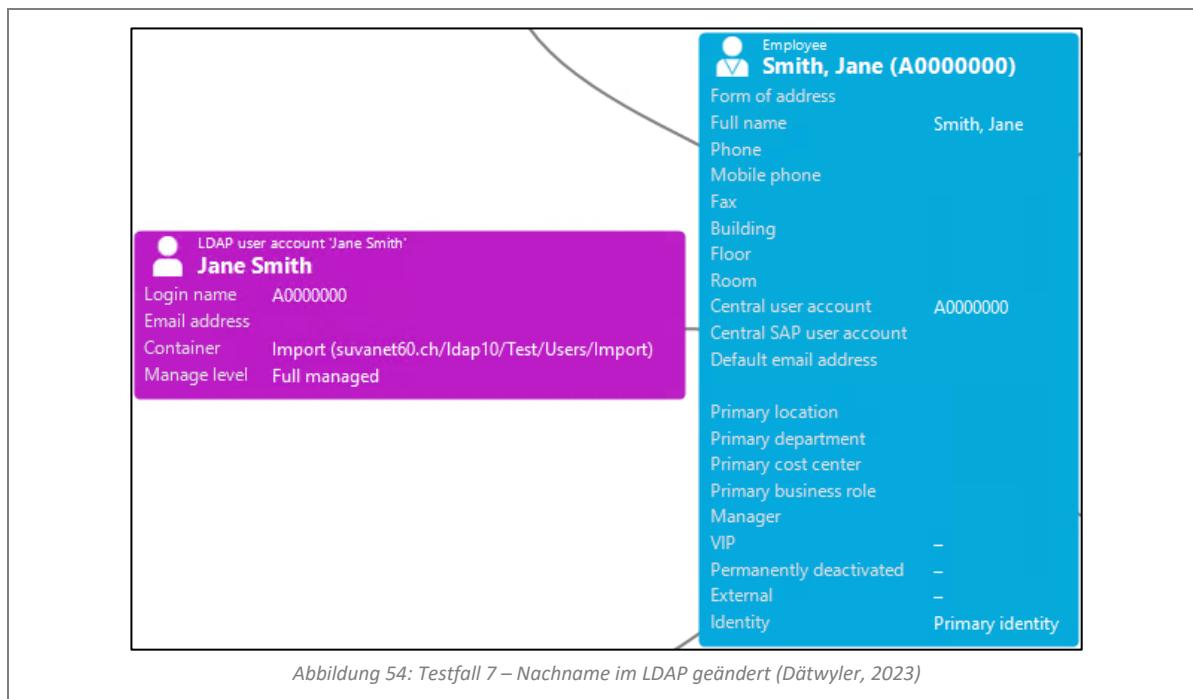


Abbildung 54: Testfall 7 – Nachname im LDAP geändert (Dätwyler, 2023)

3.5.2.7.2 Ergebnis

Auch dieses Ergebnis fiel wieder positiv aus. Die Änderung wurde vom CSV erfolgreich auf die Identität im IAM-System und dann somit auch auf den LDAP Account übertragen, wie man am obigen Bild erkennen kann.

3.5.2.8 Testfall 8: Leaver

ID	8
Bezeichnung	Leaver
Messgrösse	Identität wird deaktiviert und LDAP Account in die verzögerte Löschung aufgenommen, nachdem das Austrittsdatum der Identität = Tagesdatum gesetzt wird
Testmethode	Systemtest/Akzeptanztest manuell
Getestete Anforderung	Ziel 2 Ziel 5
Testvoraussetzung	Identity Manager in der Version 9.1 ist installiert, das CSV und das LDAP Verzeichnis wurden angehängt und der Identity Lifecycle ist implementiert.
Testmittel	<u>Identity Manager 9.1</u>
Testablauf	Ich setze im CSV das Austrittsdatum von «Jane Smith» dem Tagesdatum gleich.
Erwartetes Ergebnis	Die Identität «Jane Smith» wird deaktiviert und der dazugehörige LDAP Account wird in die verzögerte Löschung aufgenommen.

Abbildung 55: Testfall 8 (Dätwyler, 2023)

3.5.2.8.1 Durchführung

Ich öffne das CSV und setze das Austrittsdatum von «Jane Smith» dem Tagesdatum gleich.

A0000000;Jane;Smith;2017-04-20 00:00:00;2023-03-07 00:00:00

Abbildung 56: Testfall 8 – Austrittsdatum = Tagesdatum (Dätwyler, 2023)

Im **Synchronization Editor** starte ich zuerst die Simulation und danach die eigentliche Synchronisation.

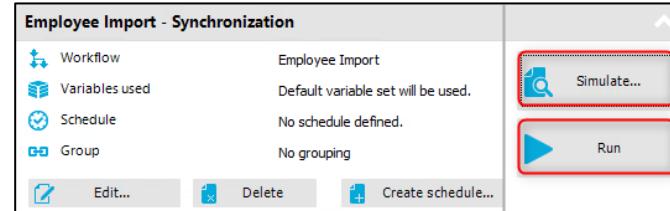


Abbildung 57: Testfall 8 – Synchronisation starten (Dätwyler, 2023)

Das Austrittsdatum wurde im IAM-System entsprechend angepasst.

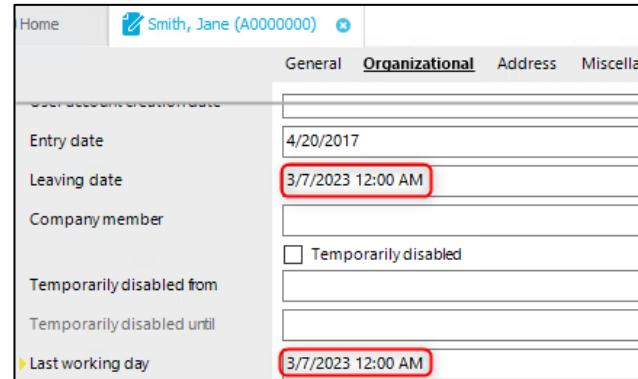


Abbildung 58: Testfall 8 – Austrittsdatum angepasst (Dätwyler, 2023)

Im **Designer** starte ich unter «Edit schedules» den Schedule «Lock accounts of employees that have left the company».

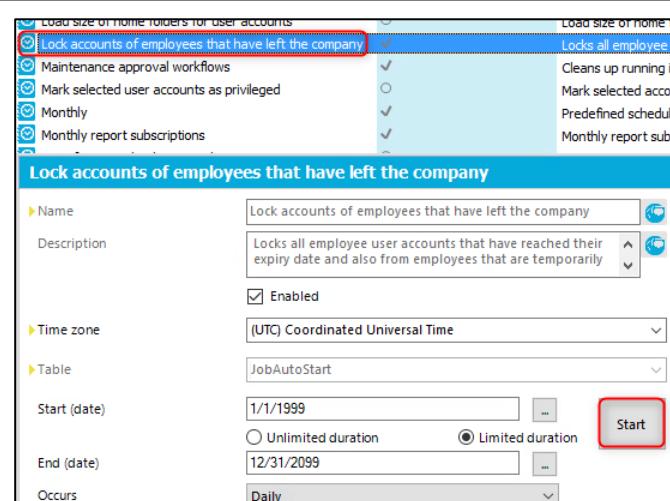


Abbildung 59: Testfall 8 – Schedule starten (Dätwyler, 2023)

Die Identität wurde permanent deaktiviert und der entsprechende Account disabled.

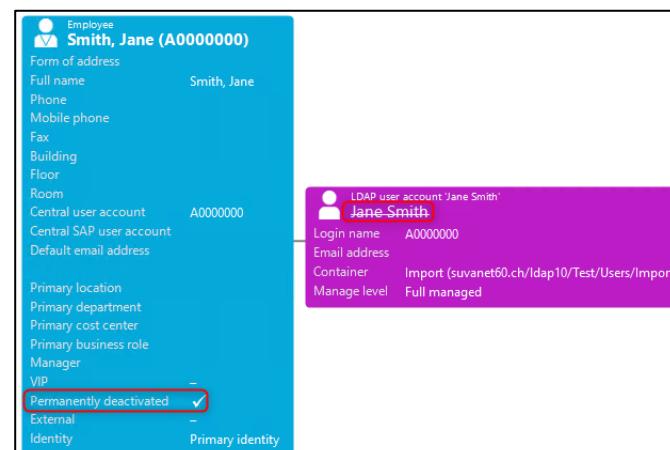
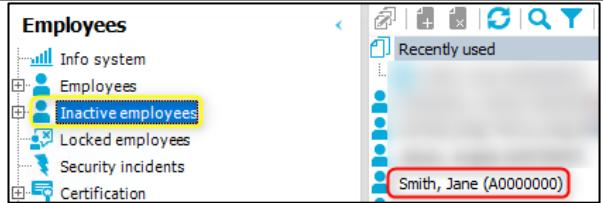
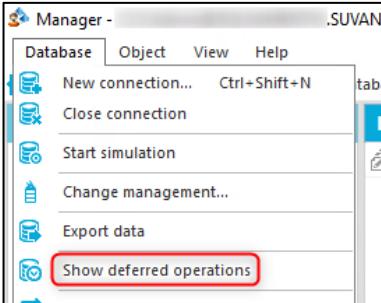
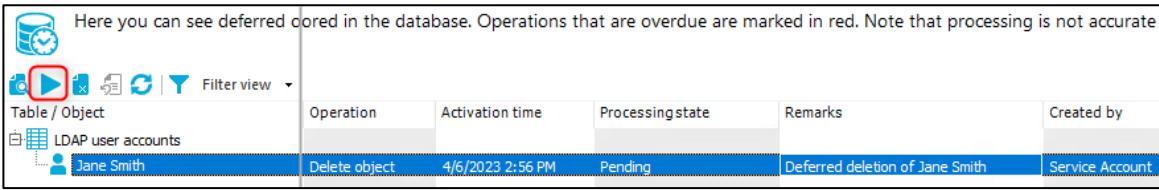


Abbildung 60: Testfall 8 – Identität und Account deaktiviert (Dätwyler, 2023)

	 <p>Abbildung 61: Testfall 8 – Identität inaktiv (Dätwyler, 2023)</p>
<p>Im Manager unter «Show deferred operations» kann die Löschung des LDAP Accounts bereits jetzt ausgeführt werden. Ansonsten wird er nach 30 Tagen automatisch gelöscht.</p>	 <p>Abbildung 62: Testfall 8 – Deferred operations (Dätwyler, 2023)</p>
 <p>Abbildung 63: Testfall 8 – LDAP Account löschen (Dätwyler, 2023)</p>	

3.5.2.8.2 Ergebnis

Die Identität wurde deaktiviert und der dazugehörige LDAP Account disabled. Aufgrund dessen wurde die Identität zu den inaktiven Personen verschoben und der LDAP Account in die verzögerte Löschung aufgenommen. Dieser letzte Testfall war somit ebenfalls ein Erfolg.

3.5.3 Testprotokoll

Um Angaben über die durchgeführten Testfälle festzuhalten, wird in diesem Testprotokoll der jeweilige Testzeitpunkt und die jeweilige Testperson niedergeschrieben.

Der Testzeitpunkt bezieht sich hierbei auf den Zeitpunkt, an dem die Durchführung beginnt.

Der Testfall 1 sowie der Testfall 5 haben keine eingetragene Zeit, da diese Testfälle nicht im Rahmen des Testings durchgeführt wurden, sondern im Rahmen der Umsetzung.

Testfall	Testzeitpunkt	Testperson
Testfall 1	28.02.2023	Mike Dätwyler
Testfall 2	07.03.2023 08:30	Mike Dätwyler
Testfall 3	07.03.2023 10:30	Mike Dätwyler
Testfall 4	07.03.2023 11:00	Mike Dätwyler
Testfall 5	01.03.2023	Mike Dätwyler
Testfall 6	07.03.2023 11:30	Mike Dätwyler
Testfall 7	07.03.2023 13:00	Mike Dätwyler
Testfall 8	07.03.2023 13:30	Mike Dätwyler

Abbildung 64: Testprotokoll (Dätwyler, 2023)

3.5.4 Testresultate

Meine Testergebnisse fielen durchwegs positiv aus – von Testfall 1 bis Testfall 8. In diesem Kapitel werden nun die Resultate der Testfälle 1 bis 8 festgehalten.

Zu sehen ist, dass alle Testfälle erfolgreich waren und mein Testing als Ganzes somit ebenfalls ein voller Erfolg war.

Testfall	Bezeichnung	Erfolgreich?
Testfall 1	.NET Installation	✓
Testfall 2	IAM System Grundfunktionalität	✓
Testfall 3	Schedules im Designer	✓
Testfall 4	Config. Parameter im Designer	✓
Testfall 5	Mitarbeiter Import mit CSV	✓
Testfall 6	Joiner	✓
Testfall 7	Mover	✓
Testfall 8	Leaver	✓

Abbildung 65: Testresultate (Dätwyler, 2023)

3.6 Auswertung – Zielkatalog

Die folgende Auswertung bezieht sich auf den erstellten Zielkatalog vom Kapitel «3.2.2.1 Zielkatalog». In diesem Zielkatalog wurden acht Muss-Kriterien und zwei Kann-Kriterien aufgestellt, welche es nun auszuwerten gilt.

Der untenstehenden Tabelle kann entnommen werden, dass alle gesetzten Muss-Kriterien erreicht wurden. Für die Kann-Kriterien konnte zeitlich gesehen kein Raum mehr geschafft werden.

ID	Muss/Kann	Bezeichnung	Erfolgreich?
1	Muss	Microsoft .NET 4.8 installieren	✓
2	Muss	Identity Manager 9.1 installieren & konfigurieren	✓
3	Muss	Alle aktiven Mitarbeiter importieren	✓
4	Muss	LDAP Verzeichnis anschliessen	✓
5	Muss	Identity Lifecycle implementieren	✓
6	Muss	Benutzeranleitung verfassen	✓
7	Muss	Big Picture der Systemarchitektur erstellen	✓
8	Muss	Suva-Standards einhalten	✓
9	Kann	Webshop Frontend installieren	✗
10	Kann	Zusätzlicher Job-Service konfigurieren	✗

Abbildung 66: Auswertung – Zielkatalog (Dätwyler, 2023)

4 Schlusswort

Die PA ist vorbei und damit neigt sich meine Lehre dem Ende zu. Ich kann sagen, dass diese PA das Anspruchsvollste meiner ganzen Lehrzeit war. Als ich immer näher zum Ende der PA kam, habe ich mich immer mehr unter Druck gesetzt, da ich dieses Dokument immer weiter ausbessern wollte. In dieser Arbeit habe ich wieder einmal gemerkt, dass ich auch nach meiner Lehre noch lange nicht ausgelernt habe. Ich freue mich jedoch auf eine Zeit, in der ich ohne schulischen Druck mein Know-how noch erweitern kann.

Am Anfang fand ich es schwer mich richtig auf die Arbeit einzustellen, da solch eine Arbeit etwas ist, dass man nicht alle Tage ausübt. Mit der Zeit ergab es sich dann aber von selbst. Dasselbe Problem kam, im kleineren Ausmass, fast jedes Mal wieder vor, wenn ich an einem neuen Kapitel angefangen habe zu schreiben. Bei der Arbeit fand ich es schwer, mich nicht von Dingen, wie das Dokument umzuformatieren oder Notizen fürs Glossar zu machen, abzulenken. Ebenfalls schwierig fand ich es, eine detaillierte Planung gleich zu Beginn zu machen. Das zeigt sich auch während der Arbeit, als ich merkte, dass ich ein paar Arbeiten zu kurz oder zu lang schätzte.

Die Installation konnte ich dann aber fehlerfrei durchführen, sodass ich darauf hin die Konfiguration ebenfalls problemlos erledigen konnte. Da diese Grundlage gegeben war, konnte ich Weiteres, wie bspw. den Mitarbeiter Export / Import, erledigen, ohne dass ich dabei grossartig anstand. Dasselbe gilt für die Anbindung des LDAPs und auch die Implementation des Identity Lifecycles. Die gewählte Lösungsvariante beim Identity Lifecycle war die richtige Entscheidung und konnte optimal umgesetzt werden. Mein Testing lief entsprechend auch recht flott und war durchgehend erfolgreich. Ich konnte alle meiner gesetzten Muss-Kriterien erreichen, was auch wieder zeigt, dass meine Arbeit sehr gut gelaufen ist. Meiner Meinung nach ist mir die Arbeit auch abseits der Umsetzung gut gelungen, denn ich habe versucht sie möglichst benutzerfreundlich zu gestalten. Ich habe nämlich ein ausführliches Abkürzungsverzeichnis sowie Glossar erstellt, Quellen jeweils im Text selbst vermerkt, stets auf meine Grammatik und Rechtschreibung geachtet und eine saubere Struktur durchs ganze Dokument gezogen.

Die detaillierte Planung half mir während der Arbeit sehr gut dabei, die Projektarbeit in greifbare Schritte zu unterteilen. Damit und in der Kombination mit Scrum, meiner angewandten Projektmanagementmethode, konnte ich den Zeitdruck optimal bewältigen. Diese PA hat mir definitiv gezeigt, was es bedeutet Zeitdruck zu haben, jedoch auch, wie man diesen entsprechend bewältigen kann. Es war teils schwer am Abend abschalten zu können, da meine Gedanken noch oft bei der Arbeit waren. Dafür hatte ich beim Arbeiten fast im Dauerzustand einen fokussierten Tunnelblick, welcher es mir ermöglichte, sehr produktiv zu arbeiten. Der erste, grösste Teil meiner PA ist nun abgeschlossen. Jetzt ist es an der Zeit mich intensiv auf die Präsentation, die Demo und das Fachgespräch vorzubereiten, damit dies reibungslos abläuft.

Ich empfand diese PA als eine überaus lehrreiche Zeit, denn sie hat mir gezeigt, wie essenziell eine genaue Planung sein kann.

Abkürzungsverzeichnis

1IM	One Identity Manager
ART	Agile Release Train
CPU	Central Processing Unit = Prozessor
CSV	Comma-separated values = Komma-getrennte Werte
DB	Datenbank / Database
DBA	Datenbank Administrator / Database Admin
GR	Geschäftsrolle
GUI	Graphical User Interface / Grafische Benutzeroberfläche
HCM	Human Capital Management
HR	Human Resources / Personalabteilung
IAM	Identity & Access Management
IDPA	Interdisziplinäre Projektarbeit
LDAP	Lightweight Directory Access Protocol
MFA	Multi Factor Authentication
MS	Microsoft
OS	Operating System = Betriebssystem
PA	praktische Arbeit
RAM	Random-Access Memory = Arbeitsspeicher
RDP	Remote Desktop Interface
RZ	Rechenzentrum
SAFe	Scaled Agile Framework
SQL	Structured Query Language
VDI	Virtual Desktop Interface

Glossar

Begriff	Definition
.exe-Datei	Die Abkürzung und Datei-Endung «exe» steht für den englischen Begriff «executable», also «ausführbar». Beim Öffnen solch einer Datei wird somit eine bestimmte Aktion ausgeführt. In der Regel bezieht sich dies auf den Start eines Programms.
.NET	.NET ist eine quelloffene Software-Plattform, die zur Entwicklung und Ausführung von Anwendungsprogrammen dient und unter der Koordination von Microsoft entwickelt wurde.
Agile Release Train (SAFe)	Ein ART ist ein auf Dauer angelegtes Team von Agile Teams, das schrittweise eine oder mehrere Lösungen bereitstellt und nach Möglichkeit betreibt.
Base object	Im Base object wird angegeben, auf welchem Job-Service die Jobs der Synchronisierung, vom Zielsystem ins IAM-System, durchlaufen. Ohne Base object im Synch Projekt ist keine Synchronisation oder Provisionierung möglich.
Big Picture	Eine Abbildung, welche einen Überblick über bspw. ein Thema oder System gibt.
Blur	Blur ist englisch und bedeutet so viel wie «verwischen». Ein Blur wird dafür verwendet, sensitive Daten aus einem Bild oder Video verschwommen und somit unkenntlich zu machen.
Configuration Parameter / Config. Parameter	Config. Parameter sind Parameter, die im Designer gesetzt werden können, um das Verhalten der Basiseinstellungen des Identity Managers zu konfigurieren.
Connection string	In der Datenverarbeitung ist ein Connection string eine Zeichenfolge, die Informationen über eine Datenquelle und die Mittel zum Herstellen einer Verbindung zu ihr angibt.
CSV-Datei	Eine CSV-Datei ist eine Textdatei, welche zur Speicherung oder zum Austausch einfach strukturierter Daten verwendet wird.
Daily (Scrum)	Das Daily Scrum ist ein tägliches Event, zu dem sich ein Team trifft, um sich gegenseitig über den Fortschritt, das Tagesziel und die bisherigen oder potenziell noch kommenden Schwierigkeiten auszutauschen.
Database owner	Mit der Database owner-Rolle können alle Konfigurations- und Wartungsaktivitäten für die Datenbank ausgeführt werden. Zudem kann mit dieser Rolle die Datenbank in SQL Server gelöscht werden.

Designer (Identity Manager Tool)	Der Designer ist das zentrale Werkzeug zur Konfiguration des Identity Managers und bietet einen Überblick über das gesamte Datenmodell des Identity Managers. Er ermöglicht die Konfiguration globaler Systemeinstellungen, wie bspw. Sprachen oder Config. Parameter, sowie die Anpassungen der Benutzeroberfläche der unterschiedlichen Administrationswerkzeuge.
Endpoint Security	Eine Endpoint Security Software ist dafür zuständig, die unterschiedlichen Endgeräte eines Netzwerks vor den unterschiedlichsten Bedrohungen zu schützen. Der unbefugte Zugriff wird durch technische und organisatorische Massnahmen verhindert.
ENTW	ENTW ist die Entwicklungsstufe der Suva. Im IAM-Umfeld dient sie fürs Testen und Entwickeln.
Epic (Scrum)	Ein Epic ist eine User Story auf höchster Abstraktionsstufe. Für einen Sprint ist sie zu gross. Der Product Owner zerlegt sie deshalb in mehrere kleinere User Stories.
Geschäftsrolle	Eine GR ist eine Bündelung von Einzelrechten, welche ein Mitarbeiter benötigt, um das Daily Business bestreiten zu können. Ein Einzelrecht kann dabei z.B. ein Zugang zu einem Programm oder System sein.
Human Capital Management / HCM-System	Ein Personalinformationssystem ist ein personenbezogenes Informationssystem, das der Erfassung, Speicherung, Verarbeitung, Pflege, Analyse, Besetzung, Verarbeitung, Übertragung und Anzeige von Informationen dient, die die Personalverwaltung betreffen.
Identity & Access Management	IAM steht für die zentrale Verwaltung von Identitäten und Zugriffsberechtigungen. Es dient als eine zentrale Zugriffskontrolle, welche jegliche Identitäten und Accounts einer Organisation, einem Netzwerk, verwaltet.
Identity Lifecycle	Identity Lifecycle bezieht sich auf den Prozess der Verwaltung von Personen/Identitäten und der Entwicklung von Zugriffsrechten von Mitarbeitern während ihrer gesamten Amtszeit. Also vom ersten Arbeitstag bis zum Austritt.
Identity Manager	Der Identity Manager ist das IAM-Produkt, welches wir in der Suva einsetzen. Dieses gehört dem Unternehmen <u>One Identity</u> .
Interdisziplinären Projektarbeit	Matura-/Abschlussarbeit in der Berufsmaturität.

INTG	INTG ist eine weitere Test-Stufe der Suva, welche zwischen ENTW und PROD liegt. Hierin können Änderungen von der ENTW transportiert werden, um zu sehen, ob der Transport funktioniert. Da die INTG quasi identisch zur Stufe PROD ist, können die Änderungen hier nochmals getestet werden und anschliessend in die PROD transportiert werden.
Job History / Process history	In der Job History des Tools JobQueueInfo können durchgelaufene Jobs nochmals angesehen, analysiert und nachvollzogen werden.
JobQueueInfo (Identity Manager)	Die JobQueueInfo liefert Unterstützung bei der Kontrolle des aktuellen Zustandes der IAM-Dienste. Es ermöglicht eine detaillierte und übersichtliche Darstellung der Aufträge/Jobs und stellt verschiedene Abfragen des Job-Services auf den Servern zur Verfügung. Das Tool liefert zudem Zustandsinformationen im laufenden Betrieb und ermöglicht eine schnelle Fehlererkennung und -suche.
Job-Server	Ein Job-Server ist ein Server, auf welchem ein Job-Service läuft. Er ist das Bindeglied zwischen den Zielsystemen und der IAM-Datenbank.
Job-Service	Der Job-Service verarbeitet alle Jobs, welche im Identity Manager abzuarbeiten sind. Zu sehen sind diese in der JobQueueInfo.
JobServiceConfigurator (Identity Manager Tool)	Mit dem JobServiceConfigurator kann man eine Konfigurationsdatei für einen Job-Service erstellen oder anpassen.
JumpVDI	Durch die JumpVDI kann man durch die Jump-Zone vom Client-Netz ins abgetrennte Server-Netz «hüpfen».
Kompilieren	Beim Kompilieren wird ein Quellcode in eine anwendbare Programmiersprache übersetzt, sodass ein Computer den Code ausführen kann.
Launchpad (Identity Manager Tool)	Das Launchpad ist das zentrale Werkzeug zum Starten der Admin-Tools des Identity Managers. Mit dem Launchpad kann man die vorhandene Identity Manager Installation prüfen und die Werkzeuge von diesem zur Ausführung einzelner Aufgaben starten.
LDAP Verzeichnis	Ein Verzeichnisdienst, wie es LDAP Verzeichnisse sind, stellt in einem Netzwerk eine zentrale Sammlung von Daten einer bestimmten Art zur Verfügung. Die in einer hierarchischen Datenbank gespeicherten Daten können verglichen, gesucht, erstellt, modifiziert und gelöscht werden.

lessons-learned	Ein lessons-learned ist ein Begriff im Projektmanagement und bedeutet so viel wie «Projekt Retrospektive».
Lightweight Directory Access Protocol	Das LDAP ist ein standardisiertes Zugriffsprotokoll, das bei Abfragen und Änderungen in Verzeichnisdiensten zum Einsatz kommt. Es gilt als Standard für Anwendungen, die mit Benutzerdaten umgehen müssten.
Log File / Log	Ein Log File enthält ein automatisch geführtes Protokoll aller oder bestimmter Aktionen von Prozessen auf einem System.
Machine role	Eine Machine role beschreibt die Rolle, die ein Computer oder Server in einem Identity Manager-System übernimmt. Man kann jedem Computer/Server mehrere Rollen zuweisen.
Manager (Identity Manager Tool)	Der Manager ist das zentrale Administrationswerkzeug zur Einrichtung aller Informationen über Personen/Identitäten. Es werden alle Informationen abgebildet und bearbeitet, die zur Verwaltung von Personen und Benutzerkonten, Berechtigungen und unternehmensspezifischen Rollen in einem IAM-Umfeld erforderlich sein.
Mapping	Das Mapping in einem Synch Projekt verbindet/mappt Attribute des Identity Managers mit den entsprechenden im Zielsystem.
Mapping Rule	Mit Mapping Rules kann man festlegen, dass z.B. alle Identitäten und Accounts mit derselben Identifikationsnummer (bei uns CentralAccount) miteinander gemappt werden sollen.
Multi Factor Authentication	MFA beschreibt das Prinzip, dass sich eine Person, welche sich an einem System authentifizieren lassen möchte, noch eine zusätzliche Authentifizierungsmethode verwenden muss. Sprich, man müsste zusätzlich zum Passwort bspw. noch eine Authenticator App verwenden.
Object Browser (Identity Manager Tool)	Mit dem Object Browser können jegliche Objekte der IAM-Datenbank eingesehen werden. Zudem ist es auch möglich, SQL-Queries zu schreiben und auszuführen.
One Identity Manager	Das war der vorherige Name des Produkts, welches mit 1IM abgekürzt wurde, bevor es zu «Identity Manager» umbenannt wurde. Aus diesem Grund findet sich diese Abkürzung auch oft noch bei Namensgebungen im IAM-Umfeld der Suva. Selbst One Identity geht noch immer nicht kontinuierlich mit dem Namen um.

Out-of-the-box-Installation	Eine Out-of-the-box-Installation ist eine Installation ohne weitere Anpassungen.
Passwort-Richtlinie	Eine Passwort-Richtlinie ist eine Reihe von Regeln, die darauf abzielen, die IT-Security zu verbessern, indem Benutzer ermutigt werden, starke Kennwörter zu verwenden und sie ordnungsgemäss zu verwenden.
persistent VDI	Hierbei verbindet sich der Benutzer immer auf die gleiche VDI. Sie bleibt dem Benutzer auch nach der Abmeldung bestehen. Es kann auch zusätzliche Software bestellt werden und persönliche Einstellungen bleiben gespeichert.
Planning (Scrum)	Bei der Sprint-Planung wird der nächste Sprint geplant, indem das Backlog mit User Stories gefüllt wird. Nach der Planung wird der geplante Sprint direkt gestartet.
private.key-File	Der Private Key ist eine separate Datei, die zur Ver- und Entschlüsselung von Daten verwendet wird, welche zwischen dem Client und dem verbundenen Server gesendet werden.
Process plan	Process plans sind mit Schedules verknüpft und können daher in regelmässigen Abständen oder bei Bedarf sofort ausgeführt werden. Zudem ist auch noch jeweils der dazugehörige Prozess verknüpft.
Process request interval	Definiert, in welchem Intervall (in Sekunden) neue Jobs abgearbeitet werden sollen.
PROD	PROD ist die Produktionsstufe der Suva. Das tägliche Arbeiten findet auf dieser Stufe statt.
Product backlog	Das Product backlog ist eine priorisierte Liste von Funktionalitäten, die ein Produkt enthalten sollte. In Scrum sind Funktionalitäten User Stories.
Product Owner (Scrum)	Der Product Owner muss fachliche Anforderungen an das Developement-Team stellen, während dann das Developement-Team diese fachlichen Anforderungen umsetzen muss. Zudem muss der Product Owner das Product backlog priorisieren.
Recovery model	Im MS SQL Management Studio kann in den Einstellungen das Recovery model auf «Full» (vollständige und differenzielle Datenbanksicherungen und Transaction-Logs möglich) oder «Simple» (vollständige und differenzielle Datenbanksicherungen möglich)
Release Notes	Release Notes sind Beschreibungen, die mit Softwareprodukten verteilt werden. Diese Versionshinweise geben meist eine grobe Übersicht über Änderungen und Verbesserungen sowie Problem-Behebungen von Softwareversionen wieder oder zeigen die Voraussetzungen für das jeweilige Produkt.

Remote Desktop Protocol	RDP ist ein sicheres Netzwerkkommunikationsprotokoll, das von <u>Microsoft</u> entwickelt wurde. Es ermöglicht den Zugriff von einem Computer auf einen anderen Computer/Server.
Role Assignment	Role Assignments können auf Role Classes konfiguriert werden. Sie geben an, welche Objekte, den sich in der Role Class befindenden GRs, angehängt werden können.
Role Class	Role Classes bilden die Grundlage für die Zuordnung von hierarchischen Rollen im Identity Manager. Sie werden verwendet, um ähnliche Rollen zu gruppieren.
Scaled Agile Framework	Das Scaled Agile Framework (SAFe) ist eine frei verfügbare Wissensbasis, mit der man Lean-Agile-Praktiken (flexibel und einfach) in einem grösseren Unternehmen anwenden kann.
Schedule	Es kommt häufig vor, dass man Prozesse und Berechnungsaufgaben im Identity Manager zu bestimmten Zeitintervallen ausführen muss. Um dies zu ermöglichen, kann man im Designer solche Zeitpläne, Schedules, definieren.
Schema Update	Durch Modifikationen oder Kompressionen ist es möglich, dass ein Schema Update bei einem Synch Projekt notwendig ist. Dies kann bspw. dann vorkommen, wenn das Schma vom Zielsystem oder vom Identity Manager angepasst wurde oder das Projekt zum ersten Mal gespeichert wird.
Scrum Master (Scrum)	Der Scrum Master unterstützt das Team darin zu wachsen, hilft dem Product Owner beim Managen des Produkts und dessen Stakeholder (Interessensgruppen) und hilft der gesamten Organisation im Verständnis und der tieferen Einführung von Scrum. Der Scrum Master muss also als Coaching-Rolle die Scrum-Methodik verinnerlichen.
Server function	Server functions entscheiden darüber, welche Prozesse bearbeitet werden können. Wenn also auf einem Job-Server die Server function «LDAP connector» deaktiviert ist, könnte man sich nicht mit einem LDAP Verzeichnis verbinden.
Service	Ein Service auf Windows ist ein Programm, das als spezialisierter Dienst im Hintergrund von Windows läuft und die Funktionalitäten des Betriebssystems oder zusätzlicher Software bündelt, um sie Dritten zur Verfügung zu stellen.

Software-Framework	Ein Software-Framework ist eine Umgebung, die Teil einer grösseren Softwareplattform ist. Es ist speziell auf die Erleichterung der Entwicklung von Softwareanwendungen ausgerichtet und das Umfassen von Komponenten wie Code-Bibliotheken, Hilfsprogrammen, Compiler, Tool-Sets und spezifische APIs, die den Datenfluss erleichtern.
Sprint (Scrum)	Ein Scrum Sprint ist ein wiederholbarer, fester Zeitrahmen. Dieser dauert meist 1 Woche. Am Ende des Sprints findet ein Review und ein Retro statt sowie die Planung des nächsten Sprints.
SQL-Query	Ein SQL-Query, ist eine Anfrage an eine Datenbank, welche in der Datensprache SQL geschrieben wird.
SQL-Where-Klausel	Der SQL-WHERE-Befehl funktioniert im Prinzip wie ein Filter, der es ermöglicht nur Datensätze anzuzeigen, die bestimmte Kriterien erfüllen. Soll also ein SQL-Query eine bestimmte Bedingung erfüllen, muss eine WHERE-Bedingung eingebaut und erfüllt werden, damit die Abfrage korrekt ausgegeben wird.
Story Point (Scrum)	Anhand von Story Points wird der Aufwand einer User Story geschätzt. Sie werden auch verwendet, um die Kapazität eines Teams für die nächsten Sprints zu schätzen. Die Länge eines Story Points kann man selbst definieren. Dies ist in der Praxis meist zwischen einer Stunde und einem Tag.
Structured Query Language	SQL ist eine Datenbanksprache zur Definition von Datenstrukturen sowie zum Bearbeiten und Abfragen von darauf basierenden Datenbeständen.
Synch Projekt	Ein Synch Projekt ist eine Sammlung aller Daten, welche für eine Synchronisation mit einem Zielsystem nötig ist. Das sind dann bspw. Base objects, Mapping oder Workflows.
Synchronization Editor / Synch Editor (Identity Manager Tool)	Die Anbindung verschiedener Zielsysteme, am Identity Manager, wird mit dem Synch Editor realisiert. Mit diesem Werkzeug konfiguriert man die Synchronisation von Daten beliebiger Zielsysteme und legt fest, welche Daten der Zielsysteme in der Identity Manager-Datenbank abgebildet werden. Dazu definiert man das Mapping der Objekteigenschaften sowie den Ablauf der Synchronisation als Workflow.
sysadmin	Mit der Rolle sysadmin kann jede Aktivität auf dem SQL Server ausgeführt werden.

Transaction Log	Ein Transaction Log ist eine Historie von ausgeführten Aktionen auf einer Datenbank. Mit der Hilfe von diesem können nach einem DB-Ausfall Datenverluste vermieden werden.
Transport-File	In einem Transport-File können bspw. Änderungen vom Designer in der ENTW exportiert und beim Designer in der INTG wieder importiert werden.
User Story (Scrum)	Eine Story ist Teil eines Epics. Sie enthält Anforderungen, geschrieben als kleine, handhabbare Texte. Auf dieser Basis schätzt das Scrum-Team den Aufwand für die Realisierung der Anforderungen ein. Wenn eine Story eine vereinbarte Zeitspanne überschreitet, kann sie in zusätzliche Stories aufgeteilt werden. Eine Story ist dann erledigt, wenn alle Aufgaben/Akzeptanzkriterien erledigt sind.
viadmin	Der viadmin ist ein Standard-Systembenutzer vom Identity Manager, welche alle Berechtigungen über die Benutzeroberfläche besitzt. <u>One Identity</u> rät dazu, ihn nicht produktiv zu verwenden. Man solle sich einen eigenen Admin erstellen.
Virtual Desktop Interface	VDI bezeichnet eine Rechenzentrum-Infrastruktur in einem Unternehmen, bei welcher komplette Desktops virtualisiert werden.
Web-GUI	Ein Web-GUI ist eine grafische Benutzeroberfläche, mit welcher man mittels eines Browsers interagieren kann.
Webshop Frontend / IT Shop (Identity Manager Tool)	Der IT Shop ist eine webbasierte Applikation für alle Identity Manager Nutzer. Über dieses Portal können unter anderem Berechtigungen/Rollen bestellt werden.
Workflow	Die Workflows in einem Synch Projekt geben an, in welche Richtung wie synchronisiert werden soll. Sprich, bspw. beim Einlesen ins IAM-System sollen die neuen Daten vom Zielsystem die im IAM-System überschreiben.

Literaturverzeichnis

- Benz, E. (2020). Abbildung 75: Floatchart – Grundlagen. *Sc04_M122_PAP03__pub0912Ashpt.pdf*. Von Sc04_M122_PAP03__pub0912Ashpt.pdf: [https://sluz.sharepoint.com/:b/r/sites/BBZW/S-INF19bL/Unterricht/Berufskunde/BK2/M122%20\(Bee\)/Lektion04/Sc04_M122_PAP03__pub0912Ashpt.pdf?csf=1&web=1&e=fpsHNA](https://sluz.sharepoint.com/:b/r/sites/BBZW/S-INF19bL/Unterricht/Berufskunde/BK2/M122%20(Bee)/Lektion04/Sc04_M122_PAP03__pub0912Ashpt.pdf?csf=1&web=1&e=fpsHNA) abgerufen
- Dätwyler, M. (2023). Abbildung 34: Testfall 2 - Test-Identität erfolgreich angelegt (Eigene Herstellung).
- Dätwyler, M. (2022). *Config. Parameter: Suva-Standard Einstellungen*. Abgerufen am 01. März 2023 von wiki.suvanet.ch: https://wiki.suvanet.ch/x/J_vIHg
- Dätwyler, M. (2023). Abbildung 1: Organigramm Suva Informatik (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 10: Arbeitsrapport – 06.03.2023 (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 11: Arbeitsrapport – 07.03.2023 (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 12: Arbeitsrapport – 08.03.2023 (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 13: Arbeitsrapport – 09.03.2023 (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 15: Zielkatalog (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 16: Systemlandschaft - Internes IAM (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 17: Identity Lifecycle (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 18: Implementationsprozess (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 19: Export – Attribut/Grund (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 2: Projektaufbauorganisation (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 20: Export – Filter/Nutzen (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 21: CSV anhängen (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 22: Base object erstellen (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 23: CSV mit Identity Manager mappen (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 24: Synchronization Workflow (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 25: Startup-Config. (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 26: CSV-Import Nachweis (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 27: LDAP-Import Nachweis (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 28: Account Definition mit Geschäftsrolle (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 29: Systemarchitektur – 1IM Standard 9.1 PA (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 3: Zeitplan (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 30: Testziele (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 31: Testfall 1 (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 32: Testfall 2 (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 33: Testfall 2 - Test-Identität anlegen (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 35: Testfall 3 (Eigene Herstellung).

- Dätwyler, M. (2023). Abbildung 36: Testfall 3 - Schedule starten (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 37: Testfall 3 - Jobs in der JobQueueInfo (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 38: Schedule starten (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 39: Jobs in der JobQueueInfo (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 4: Arbeitsrapport – 23.02.2023 (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 40: Testfall 4 (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 41: Testfall 4 - Schedule starten (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 42: Testfall 4 – «Process history» in der JobQueueInfo (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 43: Testfall 5 (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 44: Testfall 6 (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 45: Testfall 6 – Neue CSV-Zeile (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 46: Testfall 6 – Synchronisation starten (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 47: Testfall 6 – GR und Account Definition (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 48: Testfall 6 – LDAP Account erstellt (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 49: Testfall 7 (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 5: Arbeitsrapport – 24.02.2023 (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 50: Testfall 7 - Änderung im CSV (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 51: Testfall 7 – Synchronisation starten (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 52: Testfall 7: Reapply templates [1] (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 53: Testfall 7 – Reapply templates [2] (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 54: Testfall 7 – Nachname im LDAP geändert (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 55: Testfall 8 (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 56: Testfall 8 – Austrittsdatum = Tagesdatum (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 57: Testfall 8 – Synchronisation starten (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 58: Testfall 8 – Austrittsdatum angepasst (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 59: Testfall 8 – Schedule starten (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 6: Arbeitsrapport – 27.02.2023 (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 60: Testfall 8 – Identität und Account deaktiviert (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 61: Testfall 8 – Identität inaktiv (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 62: Testfall 8 – Deferred operations (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 63: Testfall 8 – LDAP Account löschen (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 64: Testprotokoll (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 65: Testresultate (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 66: Auswertung – Zielkatalog (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 67: Schedule – Process plans (Eigene Herstellung).

- Dätwyler, M. (2023). Abbildung 68: Schedule – Process plan (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 69: Backup-Archiv: OneDrive – Stand vom 01.03.2023 (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 7: Arbeitsrapport – 28.02.2023 (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 70: Backup-Archiv: Netzlaufwerk – Stand vom 01.03.2023 (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 71: Backup-Archiv: Google Drive – Stand vom 01.03.2023 (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 72: Scrum Board – Stand vom 27.02.2023 (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 73: Epic – Projektarbeit (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 74: Story – Tests auswerten (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 8: Arbeitsrapport – 01.03.2023 (Eigene Herstellung).
- Dätwyler, M. (2023). Abbildung 9: Arbeitsrapport – 02.03.2023 (Eigene Herstellung).
- habr.com. (2022). Abbildung 14: Scrum Prinzip. Abgerufen am 24. Februar 2023 von <https://habr.com/ru/company/hygger/blog/455022/>
- One Identity. (2023). *Identity Manager 9.1 - Release Notes*. Abgerufen am 1. März 2023 von support.oneidentity.com: <https://support.oneidentity.com/technical-documents/identitymanager/9.1/release-notes/3#TOPIC-1864568>
- Stadelmann, A. (2023). *Security Einstellungen und Passwort Richtlinien ab V.8.x*. Abgerufen am 01. März 2023 von wiki.suvanet.ch: <https://wiki.suvanet.ch/x/aoS8EQ>
- Suva. (2022). *Die Suva*. Abgerufen am 21. Oktober 2022 von suva.ch: <https://www.suva.ch/dech/die-suva/ueber-uns/die-suva>
- Vogt, O. (2016). *Installationsanleitung Dell One Identity Manager inkl History DB und HotFixes*. Abgerufen am 28. Februar 2023 von wiki.suvanet.ch: <https://wiki.suvanet.ch/x/7Z0-CQ>
- Vogt, O. (2016). *Installationsanleitung One Identity Manager Version 7.1.0*. Abgerufen am 28. Februar 2023 von wiki.suvanet.ch: <https://wiki.suvanet.ch/x/xI-TCQ>
- Vogt, O. (2022). *Datenbank verschlüsseln*. Abgerufen am 28. Februar 2023 von wiki.suvanet.ch: <https://wiki.suvanet.ch/x/7JQ-CQ>

Abbildungsverzeichnis

Abbildung 1: Organigramm – Suva Informatik (Dätwyler, 2023).....	6
Abbildung 2: Projektaufbauorganisation (Dätwyler, 2023)	7
Abbildung 3: Zeitplan (Dätwyler, 2023)	10
Abbildung 4: Arbeitsrapport – 23.02.2023 (Dätwyler, 2023).....	11
Abbildung 5: Arbeitsrapport – 24.02.2023 (Dätwyler, 2023).....	12
Abbildung 6: Arbeitsrapport – 27.02.2023 (Dätwyler, 2023).....	13
Abbildung 7: Arbeitsrapport – 28.02.2023 (Dätwyler, 2023).....	14
Abbildung 8: Arbeitsrapport – 01.03.2023 (Dätwyler, 2023).....	15
Abbildung 9: Arbeitsrapport – 02.03.2023 (Dätwyler, 2023).....	16
Abbildung 10: Arbeitsrapport – 06.03.2023 (Dätwyler, 2023).....	17
Abbildung 11: Arbeitsrapport – 07.03.2023 (Dätwyler, 2023).....	18
Abbildung 12: Arbeitsrapport – 08.03.2023 (Dätwyler, 2023).....	19
Abbildung 13: Arbeitsrapport – 09.03.2023 (Dätwyler, 2023).....	20
Abbildung 14: Scrum Prinzip (habr.com, 2022).....	24
Abbildung 15: Zielkatalog (Dätwyler, 2023)	26
Abbildung 16: Systemlandschaft – Internes IAM (Dätwyler, 2023)	28
Abbildung 17: Identity Lifecycle (Dätwyler, 2023)	29
Abbildung 18: Implementationsprozess (Dätwyler, 2023).....	31
Abbildung 19: Export – Attribut/Grund (Dätwyler, 2023).....	33
Abbildung 20: Export – Filter/Nutzen (Dätwyler, 2023).....	33
Abbildung 21: CSV anhängen (Dätwyler, 2023)	33
Abbildung 22: Base object erstellen (Dätwyler, 2023).....	34
Abbildung 23: CSV mit Identity Manager mappen (Dätwyler, 2023).....	34
Abbildung 24: Synchronization Workflow (Dätwyler, 2023).....	34
Abbildung 25: Startup-Config. (Dätwyler, 2023)	35
Abbildung 26: CSV-Import Nachweis (Dätwyler, 2023).....	35
Abbildung 27: LDAP-Import Nachweis (Dätwyler, 2023)	35
Abbildung 28: Account Definition mit Geschäftsrolle (Dätwyler, 2023)	36
Abbildung 29: Systemarchitektur – 1IM Standard 9.1 PA (Dätwyler, 2023)	38
Abbildung 30: Testziele (Dätwyler, 2023)	39
Abbildung 31: Testfall 1 (Dätwyler, 2023).....	40
Abbildung 32: Testfall 2 (Dätwyler, 2023).....	40
Abbildung 33: Testfall 2 – Test-Identität anlegen (Dätwyler, 2023)	41
Abbildung 34: Testfall 2 – Test-Identität erfolgreich angelegt (Dätwyler, 2023)	41
Abbildung 35: Testfall 3 (Dätwyler, 2023).....	42
Abbildung 36: Testfall 3 – Schedule starten (Dätwyler, 2023)	42

Abbildung 37: Testfall 3 – Jobs in der JobQueueInfo (Dätwyler, 2023)	42
Abbildung 38: Schedule starten (Dätwyler, 2023)	43
Abbildung 39: Jobs in der JobQueueInfo (Dätwyler, 2023).....	43
Abbildung 40: Testfall 4 (Dätwyler, 2023).....	43
Abbildung 41: Testfall 4 – Schedule starten (Dätwyler, 2023).....	44
Abbildung 42: Testfall 4 – «Process history» in der JobQueueInfo (Dätwyler, 2023).....	44
Abbildung 43: Testfall 5 (Dätwyler, 2023).....	45
Abbildung 44: Testfall 6 (Dätwyler, 2023).....	45
Abbildung 45: Testfall 6 – Neue CSV-Zeile (Dätwyler, 2023)	46
Abbildung 46: Testfall 6 – Synchronisation starten (Dätwyler, 2023).....	46
Abbildung 47: Testfall 6 – GR und Account Definition (Dätwyler, 2023)	46
Abbildung 48: Testfall 6 – LDAP Account erstellt (Dätwyler, 2023)	47
Abbildung 49: Testfall 7 (Dätwyler, 2023).....	47
Abbildung 50: Testfall 7 – Änderung im CSV (Dätwyler, 2023)	47
Abbildung 51: Testfall 7 – Synchronisation starten (Dätwyler, 2023).....	48
Abbildung 52: Testfall 7: Reapply templates [1] (Dätwyler, 2023)	48
Abbildung 53: Testfall 7 – Reapply templates [2] (Dätwyler, 2023).....	48
Abbildung 54: Testfall 7 – Nachname im LDAP geändert (Dätwyler, 2023).....	49
Abbildung 55: Testfall 8 (Dätwyler, 2023).....	49
Abbildung 56: Testfall 8 – Austrittsdatum = Tagesdatum (Dätwyler, 2023)	49
Abbildung 57: Testfall 8 – Synchronisation starten (Dätwyler, 2023).....	50
Abbildung 58: Testfall 8 – Austrittsdatum angepasst (Dätwyler, 2023)	50
Abbildung 59: Testfall 8 – Schedule starten (Dätwyler, 2023).....	50
Abbildung 60: Testfall 8 – Identität und Account deaktiviert (Dätwyler, 2023)	50
Abbildung 61: Testfall 8 – Identität inaktiv (Dätwyler, 2023)	51
Abbildung 62: Testfall 8 – Deferred operations (Dätwyler, 2023)	51
Abbildung 63: Testfall 8 – LDAP Account löschen (Dätwyler, 2023)	51
Abbildung 64: Testprotokoll (Dätwyler, 2023)	51
Abbildung 65: Testresultate (Dätwyler, 2023)	52
Abbildung 66: Auswertung – Zielkatalog (Dätwyler, 2023).....	52
Abbildung 67: Schedule – Process plans (Dätwyler, 2023)	68
Abbildung 68: Schedule – Process plan (Dätwyler, 2023).....	73
Abbildung 69: Backup-Archiv: OneDrive – Stand vom 01.03.2023 (Dätwyler, 2023)	74
Abbildung 70: Backup-Archiv: Netzlaufwerk – Stand vom 01.03.2023 (Dätwyler, 2023).....	74
Abbildung 71: Backup-Archiv: Google Drive – Stand vom 01.03.2023 (Dätwyler, 2023)	74
Abbildung 72: Scrum Board – Stand vom 27.02.2023 (Dätwyler, 2023).....	75
Abbildung 73: Epic – Projektarbeit (Dätwyler, 2023).....	76
Abbildung 74: Story – Tests auswerten (Dätwyler, 2023).....	76
Abbildung 75: Floatchart – Grundlagen (Benz, 2020)	77

Anhang

Schedules – Log Files

Daily maintenance tasks

Schedule-Aufbau

Die abgebildeten Process plans sind im Log File aufzufinden. Dadurch ist der Durchlauf des Jobs bewiesen.

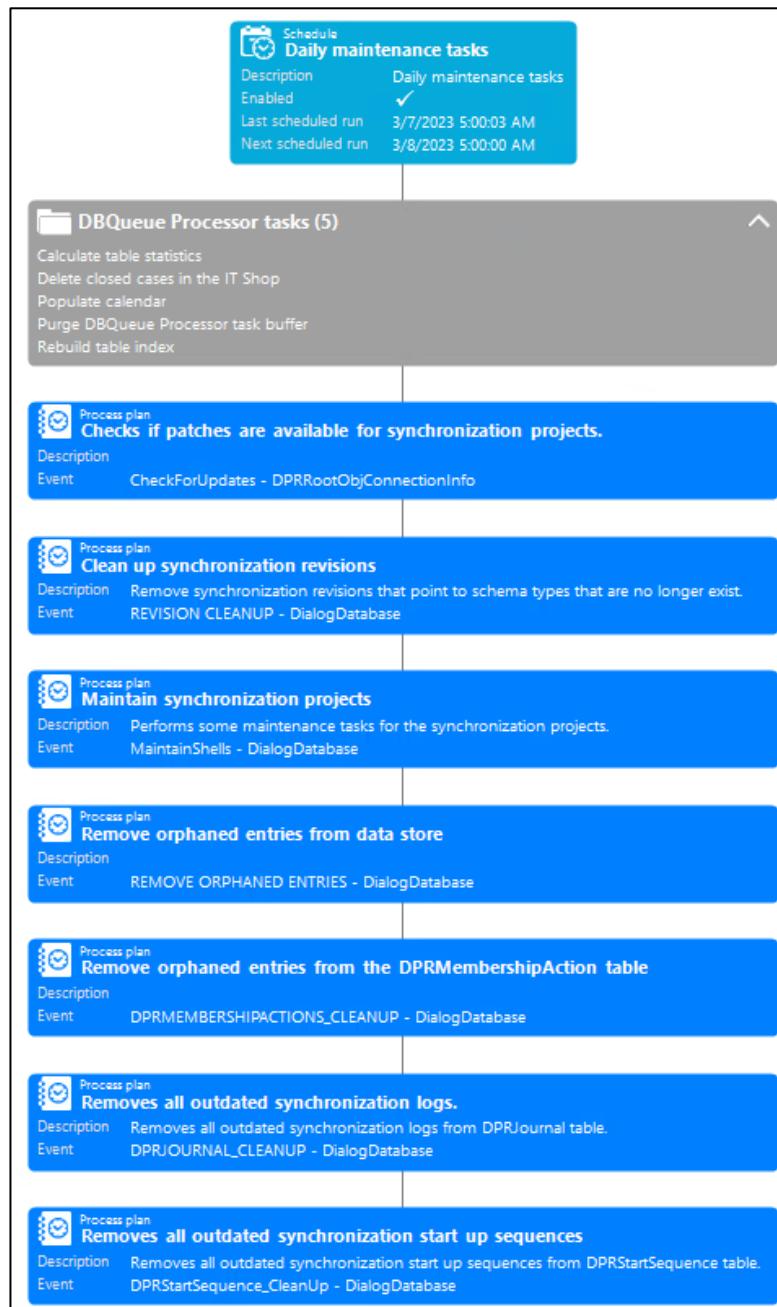


Abbildung 67: Schedule – Process plans (Dätwyler, 2023)

Log File

2023-03-07 10:45:53 +01:00 - Parameters - \JOBSERVICE01 -
 Process step parameter BED83FA0-EFA9-4C03-9A09-
 96CBA2577DD7:
 [Job]
 ComponentAssembly=HandleObjectComponent
 ComponentClass=VI.JobService.JobComponents.H
 andleObjectComponent
 Task=FireGenEvent
 Executiontype=INTERNAL
 [Parameters]
 ConnectionProvider=VI.DB.ViSqlFactory,VI.DB
 ConnectionString=Hidden
 EventName=DPRMEMBERSHIPACTIONS_CLEANU
 P
 objecttype=DialogDatabase
 ProID=531E05F8-41E4-4074-8951-
 3421AD1947BB
 WhereClause=XObjectKey in
 ('<Key><T>DialogDatabase</T><P>1750ADFO-107A-47FB-
 8ECC-E305080B45D4</P></Key>')
 _paramName1=StopTime
 _paramValue1=2200-01-01 00:00:00.000
 2023-03-07 10:45:53 +01:00 - Info: Last process step
 request succeeded.
 2023-03-07 10:45:53 +01:00 - Parameters - \JOBSERVICE01 -
 Process step parameter 339B748E-4CC0-41B4-8CA5-
 37B12082FD8E:
 [Job]
 ComponentAssembly=HandleObjectComponent
 ComponentClass=VI.JobService.JobComponents.H
 andleObjectComponent
 Task=FireGenEvent
 Executiontype=INTERNAL
 [Parameters]
 ConnectionProvider=VI.DB.ViSqlFactory,VI.DB
 ConnectionString=Hidden
 EventName=DPRStartSequence_CleanUp
 objecttype=DialogDatabase
 ProID=298C3E86-BB2D-4208-9CED-
 AED94C18B9AC
 WhereClause=XObjectKey in
 ('<Key><T>DialogDatabase</T><P>1750ADFO-107A-47FB-
 8ECC-E305080B45D4</P></Key>')
 _paramName1=StopTime
 _paramValue1=2200-01-01 00:00:00.000
 2023-03-07 10:45:53 +01:00 - Parameters - \JOBSERVICE01 -
 Process step parameter 290F5906-3307-478F-A373-
 9DA50BB0B044:
 [Job]
 ComponentAssembly=HandleObjectComponent
 ComponentClass=VI.JobService.JobComponents.H
 andleObjectComponent
 Task=FireGenEvent
 Executiontype=INTERNAL
 [Parameters]
 ConnectionProvider=VI.DB.ViSqlFactory,VI.DB
 ConnectionString=Hidden
 EventName=MaintainShells
 objecttype=DialogDatabase
 ProID=C11D9B7F-8B4B-40BF-B712-
 558DE3958447
 WhereClause=XObjectKey in
 ('<Key><T>DialogDatabase</T><P>1750ADFO-107A-47FB-
 8ECC-E305080B45D4</P></Key>')
 _paramName1=StopTime
 _paramValue1=2200-01-01 00:00:00.000
 2023-03-07 10:45:53 +01:00 - Info: Loading configuration
 parameters...
 2023-03-07 10:45:53 +01:00 - Parameters - \JOBSERVICE01 -
 Process step parameter E5319F64-F965-45AE-95CB-
 631EAA079097:
 [Job]
 ComponentAssembly=HandleObjectComponent
 ComponentClass=VI.JobService.JobComponents.H
 andleObjectComponent
 Task=FireGenEvent
 Executiontype=INTERNAL
 [Parameters]
 ConnectionProvider=VI.DB.ViSqlFactory,VI.DB
 ConnectionString=Hidden
 EventName=CheckForUpdates
 objecttype=DPRRootObjConnectionInfo
 ProID=ADEE8BC6-0EA7-42B3-88F0-
 A296E1B3C59F
 WhereClause=XObjectKey in
 ('<Key><T>DPRRootObjConnectionInfo</T><P>994f0199-
 c8fa-4e1c-a0a3-
 38e178fc25d9</P></Key>','<Key><T>DPRRootObjConnectio
 nInfo</T><P>bdb70684-3007-467d-a5c5-
 f0edc95a0696</P></Key>')
 _paramName1=StopTime
 _paramValue1=2200-01-01 00:00:00.000
 2023-03-07 10:45:54 +01:00 - Parameters - \JOBSERVICE01 -
 Process step parameter 686CB815-38E7-49BB-A0A3-
 3F1202BE3A46:
 [Job]
 ComponentAssembly=HandleObjectComponent
 ComponentClass=VI.JobService.JobComponents.H
 andleObjectComponent
 Task=FireGenEvent
 Executiontype=INTERNAL
 [Parameters]
 ConnectionProvider=VI.DB.ViSqlFactory,VI.DB
 ConnectionString=Hidden
 EventName=DPRJOURNAL_CLEANUP
 objecttype=DialogDatabase
 ProID=6B78A433-5DC8-4AE6-961D-
 E2AAABFA54BA
 WhereClause=XObjectKey in
 ('<Key><T>DialogDatabase</T><P>1750ADFO-107A-47FB-
 8ECC-E305080B45D4</P></Key>')
 _paramName1=StopTime
 _paramValue1=2200-01-01 00:00:00.000
 2023-03-07 10:45:54 +01:00 - Success - \JOBSERVICE01 -

VI.JobService.JobComponents.HandleObjectComponent - 339B748E-4CC0-41B4-8CA5-37B12082FDBE: Successful
The event DPRStartSequence_CleanUp was triggered for 1 object(s) of type DialogDatabase.
2023-03-07 10:45:54 +01:00 - Success - \JOBSERVICE01 - VI.JobService.JobComponents.HandleObjectComponent - 290F5906-3307-478F-A373-9DA50BB0B044: Successful
The event MaintainShells was triggered for 1 object(s) of type DialogDatabase.
2023-03-07 10:45:54 +01:00 - Info: Requesting process steps for queue "\JOBSERVICE01".
2023-03-07 10:45:54 +01:00 - Parameters - \JOBSERVICE01 - Process step parameter C88C3F9E-FA8A-4314-8FEB-3C98DD1DB4E7:
[Job]
ComponentAssembly=HandleObjectComponent
ComponentClass=VI.JobService.JobComponents.HandleObjectComponent
Task=FireGenEvent
Executiontype=INTERNAL
[Parameters]
ConnectionProvider=VI.DB.ViSqlFactory,VI.DB
ConnectionString=Hidden
EventName=REVISION CLEANUP
objecttype=DialogDatabase
ProcID=2E9F635F-2E05-4118-9770-5B5E427F6261
WhereClause=XObjectKey in ('<Key><T>DialogDatabase</T><P>1750ADF0-107A-47FB-8ECC-E305080B45D4</P></Key>')
_paramName1=StopTime
_paramValue1=2200-01-01 00:00:00.000
2023-03-07 10:45:54 +01:00 - Success - \JOBSERVICE01 - VI.JobService.JobComponents.HandleObjectComponent - BED83FA0-EFA9-4C03-9A09-96CBA2577DD7: Successful
The event DPRMEMBERSHIPACTIONS_CLEANUP was triggered for 1 object(s) of type DialogDatabase.
2023-03-07 10:45:54 +01:00 - Parameters - \JOBSERVICE01 - Process step parameter A77C93CC-C963-4CA7-AE71-2546A5E21F7C:
[Job]
ComponentAssembly=HandleObjectComponent
ComponentClass=VI.JobService.JobComponents.HandleObjectComponent
Task=FireGenEvent
Executiontype=INTERNAL
[Parameters]
ConnectionProvider=VI.DB.ViSqlFactory,VI.DB
ConnectionString=Hidden
EventName=REMOVE ORPHANED ENTRIES
objecttype=DialogDatabase
ProcID=521E1E88-D542-42A4-9D8E-998CB0AE0CEE
WhereClause=XObjectKey in ('<Key><T>DialogDatabase</T><P>1750ADF0-107A-47FB-8ECC-E305080B45D4</P></Key>')
_paramName1=StopTime
_paramValue1=2200-01-01 00:00:00.000
2023-03-07 10:45:54 +01:00 - Success - \JOBSERVICE01 - VI.JobService.JobComponents.HandleObjectComponent - 686CB815-38E7-49BB-A0A3-3F1202BE3A46: Successful
The event DPRJOURNAL_CLEANUP was triggered for 1 object(s) of type DialogDatabase.
2023-03-07 10:45:54 +01:00 - Info: Last process step request succeeded.
2023-03-07 10:45:54 +01:00 - Success - \JOBSERVICE01 - VI.JobService.JobComponents.HandleObjectComponent - C88C3F9E-FA8A-4314-8FEB-3C98DD1DB4E7: Successful
The event REVISION CLEANUP was triggered for 1 object(s) of type DialogDatabase.
2023-03-07 10:45:54 +01:00 - Success - \JOBSERVICE01 - VI.JobService.JobComponents.HandleObjectComponent - E5319F64-F965-45AE-95CB-631EAA079097: Successful
The event CheckForUpdates was triggered for 2 object(s) of type DPRRootObjConnectionInfo.
2023-03-07 10:45:54 +01:00 - Parameters - \JOBSERVICE01 - Process step parameter 4cec3dc9-1261-4754-8a6c-951a16c971af:
[Job]
ComponentAssembly=HandleObjectComponent
ComponentClass=VI.JobService.JobComponents.HandleObjectComponent
Task=FireGenEvent
Executiontype=INTERNAL
[Parameters]
AuthenticationString=Hidden
ConnectionProvider=VI.DB.ViSqlFactory,VI.DB
ConnectionString=Hidden
EventName=Maintain
ObjectType=DPRShell
ProcID=C11D9B7F-8B4B-40BF-B712-558DE3958447
StopTime=Hidden
2023-03-07 10:45:54 +01:00 - Success - \JOBSERVICE01 - VI.JobService.JobComponents.HandleObjectComponent - A77C93CC-C963-4CA7-AE71-2546A5E21F7C: Successful
The event REMOVE ORPHANED ENTRIES was triggered for 1 object(s) of type DialogDatabase.
2023-03-07 10:45:54 +01:00 - Parameters - \JOBSERVICE01 - Process step parameter dfa8a82c-3e74-413c-8a4b-f6dfe34c2942:
[Job]
ComponentAssembly=SQLComponent
ComponentClass=VI.JobService.JobComponents.SQLComponent
Task=Execute SQL
Executiontype=INTERNAL
[Parameters]
ConnectionProvider=VI.DB.ViSqlFactory,VI.DB
ConnectionString=Hidden
ProcID=298C3E86-BB2D-4208-9CED-AED94C18B9AC
SQLStmt=exec QBM_PDeleteBulk N'DPRStartSequence', N'(UID_DPRStartSequenceTemplate > '' '') and (isnull(XDateUpdated, "1899-12-30 00:00:00.000") < "2023-02-28 09:45:54.013") and (ExecutionState in (N"Error", N"Processed"))'
StopTime=Hidden

2023-03-07 10:45:54 +01:00 - Info: Requesting process steps for queue "\JOBSERVICE01".

2023-03-07 10:45:54 +01:00 - Parameters - \JOBSERVICE01 - Process step parameter 7923fe92-bbef-4564-a7d6-95265a7eb911:

[Job]

- ComponentAssembly=SQLComponent
- ComponentClass=VI.JobService.JobComponents.SQLComponent
- Task=Execute SQL
- Executiontype=INTERNAL

[Parameters]

- ConnectionProvider=VI.DB.ViSqlFactory,VI.DB
- ConnectionString=Hidden
- ProID=531E05F8-41E4-4074-8951-3421AD1947BB

SQLStmt=exec DPR_PMemberShipActionCleanUp

StopTime=Hidden

2023-03-07 10:45:54 +01:00 - Success - \JOBSERVICE01 - VI.JobService.JobComponents.HandleObjectComponent - 4cec3dc9-1261-4754-8a6c-951a16c971af: Successful

The event Maintain was triggered for 2 object(s) of type DPRShell.

2023-03-07 10:45:54 +01:00 - Parameters - \JOBSERVICE01 - Process step parameter 2e024687-6bbd-4507-afa2-ffec793f700:

[Job]

- ComponentAssembly=SQLComponent
- ComponentClass=VI.JobService.JobComponents.SQLComponent
- Task=Execute SQL
- Executiontype=INTERNAL

[Parameters]

- ConnectionProvider=VI.DB.ViSqlFactory,VI.DB
- ConnectionString=Hidden
- ProID=6B78A433-5DC8-4AE6-961D-E2AAABFA54BA

SQLStmt=exec QBM_PDeleteBulk N'DPRJournal', N'(isnull(CreationTime, "1899-12-30 00:00:00.000") < "2023-02-05 09:45:54.044") and (isnull(ProjectionState, N'") <> N"Running")'

StopTime=Hidden

WithoutTransaction=True

2023-03-07 10:45:54 +01:00 - Info: Last process step request succeeded.

2023-03-07 10:45:54 +01:00 - Parameters - \JOBSERVICE01 - Process step parameter 050363f7-d712-436d-a6d1-8773e4187d06:

[Job]

- ComponentAssembly=VI.Projector.JobComponent
- ComponentClass=VI.Projector.JobComponent.ProjectorComponent
- Task=MigrationStateAnalysis
- Executiontype=EXTERNAL

[Parameters]

- AuthenticationString=Hidden
- ConnectionProvider=VI.DB.ViSqlFactory,VI.DB
- ConnectionString=Hidden

ProcID=ADEE8BC6-0EA7-42B3-88F0-A296E1B3C59F

StopTime=Hidden

UID_DPRShell=CCC-3B0664FFD76B7649A2EFB5A44A9B94F5

2023-03-07 10:45:54 +01:00 - Success - \JOBSERVICE01 - VI.JobService.JobComponents.SQLComponent - 7923fe92-bbef-4564-a7d6-95265a7eb911: Successful

2023-03-07 10:45:54 +01:00 - Success - \JOBSERVICE01 - VI.JobService.JobComponents.SQLComponent - 2e024687-6bbd-4507-afa2-ffec793f700: Successful

2023-03-07 10:45:54 +01:00 - Success - \JOBSERVICE01 - VI.JobService.JobComponents.SQLComponent - dfa8a82c-3e74-413c-8a4b-f6dfe34c2942: Successful

2023-03-07 10:45:54 +01:00 - Parameters - \JOBSERVICE01 - Process step parameter 6a268971-8a67-4a7c-8c93-f8446376c744:

[Job]

- ComponentAssembly=SQLComponent
- ComponentClass=VI.JobService.JobComponents.SQLComponent
- Task=Execute SQL
- Executiontype=INTERNAL

[Parameters]

- ConnectionProvider=VI.DB.ViSqlFactory,VI.DB
- ConnectionString=Hidden
- ProID=2E9F635F-2E05-4118-9770-5B5E427F6261

SQLStmt=delete DPRRevisionStore

where SchemaTypeKey not in (

- select 'Schema['+s.SystemId+'].Type['+st.Name+']' from DPRSchemaType st join DPRSchema s on st.UID_DPRSchema = s.UID_DPRSchema)

StopTime=Hidden

2023-03-07 10:45:54 +01:00 - Parameters - \JOBSERVICE01 - Process step parameter d1accd8d-5c6a-47d8-841e-5611433e73be:

[Job]

- ComponentAssembly=SQLComponent
- ComponentClass=VI.JobService.JobComponents.SQLComponent
- Task=Execute SQL
- Executiontype=INTERNAL

[Parameters]

- ConnectionProvider=VI.DB.ViSqlFactory,VI.DB
- ConnectionString=Hidden
- ProID=521E1E88-D542-42A4-9D8E-998CB0AE0CEE

SQLStmt=exec DPR_PAttachedDataStoreCleanUp

StopTime=Hidden

2023-03-07 10:45:54 +01:00 - Parameters - \JOBSERVICE01 - Process step parameter e1ffe8c9-b92d-4810-a3be-2329bbaf08fc:

[Job]

- ComponentAssembly=VI.Projector.JobComponent
- ComponentClass=VI.Projector.JobComponent.ProjectorComponent

```

jectorComponent
  Task=MaintainShell
  Executiontype=EXTERNAL
[Parameters]
  AuthenticationString=Hidden
  ConnectionProvider=VI.DB.ViSqlFactory,VI.DB
  ConnectionString=Hidden
  ProclD=C11D9B7F-8B4B-40BF-B712-
558DE3958447
  UID_DPRShell=CCC-
3B0664FFD76B7649A2EFB5A44A9B94F5
2023-03-07 10:45:54 +01:00 - Success - \JOBSERVICE01 -
VI.JobService.JobComponents.SQLComponent - 6a268971-
8a67-4a7c-8c93-f8446376c744: Successful
2023-03-07 10:45:54 +01:00 - Success - \JOBSERVICE01 -
VI.JobService.JobComponents.SQLComponent - d1accd8d-
5c6a-47d8-841e-5611433e73be: Successful
2023-03-07 10:45:55 +01:00 - Info: Loading configuration
parameters...
2023-03-07 10:45:55 +01:00 - Info: Loading configuration
parameters...
2023-03-07 10:45:55 +01:00 - Info: Loading script assembly
WebServices_7bQd6FbE4ufgluWnni6lWFModWoCSV5 from
local cache.
2023-03-07 10:45:55 +01:00 - Info: Loading script assembly
TypedWrappers_7bQd6FbE4ufgluWnni6lWFModWoCSV5
from local cache.
2023-03-07 10:45:55 +01:00 - Info: Loading script assembly
ProductScripts_7bQd6FbE4ufgluWnni6lWFModWoCSV5
from local cache.
2023-03-07 10:45:55 +01:00 - Info: Loading script assembly
Scripts_7bQd6FbE4ufgluWnni6lWFModWoCSV5 from local
cache.
2023-03-07 10:45:55 +01:00 - Info: Loading script assembly
WebServices_7bQd6FbE4ufgluWnni6lWFModWoCSV5 from
local cache.
2023-03-07 10:45:55 +01:00 - Info: Loading script assembly
TypedWrappers_7bQd6FbE4ufgluWnni6lWFModWoCSV5
from local cache.
2023-03-07 10:45:55 +01:00 - Info: Loading script assembly
ProductScripts_7bQd6FbE4ufgluWnni6lWFModWoCSV5
from local cache.
2023-03-07 10:45:55 +01:00 - Info: Loading script assembly
Scripts_7bQd6FbE4ufgluWnni6lWFModWoCSV5 from local
cache.
2023-03-07 10:45:56 +01:00 - Success - \JOBSERVICE01 -
VI.Projector.JobComponent.ProjectorComponent -
e1ffe8c9-b92d-4810-a3be-2329bbaf08fc: Successful
2023-03-07 10:46:01 +01:00 - Success - \JOBSERVICE01 -
VI.Projector.JobComponent.ProjectorComponent -
050363f7-d712-436d-a6d1-8773e4187d06: Successful
2023-03-07 10:46:01 +01:00 - Info: Requesting process
steps for queue "\JOBSERVICE01".
2023-03-07 10:46:01 +01:00 - Parameters - \JOBSERVICE01 -
Process step parameter a07d17c8-89ee-4947-b59f-
7bfe9bf79294:
[Job]
  ComponentAssembly=VI.Projector.JobComponen
t
  ComponentClass=VI.Projector.JobComponent.Pro
jectorComponent
  Task=MigrationStateAnalysis
  Executiontype=EXTERNAL
[Parameters]
  AuthenticationString=Hidden
  ConnectionProvider=VI.DB.ViSqlFactory,VI.DB
  ConnectionString=Hidden
  ProclD=ADEE8BC6-0EA7-42B3-88F0-
A296E1B3C59F
  StopTime=Hidden
  UID_DPRShell=CCC-
3D08FF659AE06F4CA75A7366D89A6A05
2023-03-07 10:46:01 +01:00 - Info: Last process step
request succeeded.
2023-03-07 10:46:01 +01:00 - Info: Requesting process
steps for queue "\JOBSERVICE01".
2023-03-07 10:46:01 +01:00 - Parameters - \JOBSERVICE01 -
Process step parameter 2e3adde3-8d57-40bb-b095-
1725e9fa1405:
[Job]
  ComponentAssembly=VI.Projector.JobComponen
t
  ComponentClass=VI.Projector.JobComponent.Pro
jectorComponent
  Task=MaintainShell
  Executiontype=EXTERNAL
[Parameters]
  AuthenticationString=Hidden
  ConnectionProvider=VI.DB.ViSqlFactory,VI.DB
  ConnectionString=Hidden
  ProclD=C11D9B7F-8B4B-40BF-B712-
558DE3958447
  UID_DPRShell=CCC-
3D08FF659AE06F4CA75A7366D89A6A05
2023-03-07 10:46:01 +01:00 - Info: Last process step
request succeeded.
2023-03-07 10:46:01 +01:00 - Success - \JOBSERVICE01 -
VI.Projector.JobComponent.ProjectorComponent -
2e3adde3-8d57-40bb-b095-1725e9fa1405: Successful
2023-03-07 10:46:03 +01:00 - Success - \JOBSERVICE01 -
VI.Projector.JobComponent.ProjectorComponent -
a07d17c8-89ee-4947-b59f-7bfe9bf79294: Successful
2023-03-07 10:46:08 +01:00 - Info: Requesting process
steps for queue "\JOBSERVICE01".

```

Updates current UTC offsets for all time zones

Schedule-Aufbau

Der abgebildete Process plan ist im Log File aufzufinden. Dadurch ist der Durchlauf des Jobs bewiesen.

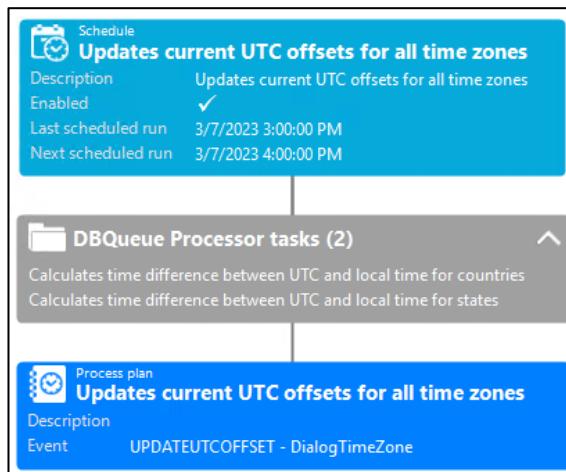


Abbildung 68: Schedule – Process plan (Dätwyler, 2023)

Log File

```

2023-03-07 10:51:09 +01:00 - Parameters - \JOBSERVICE01 -
Process step parameter 243B18E6-7F33-4784-AEBO-
3DE7912D5D55:
[Job]
    ComponentAssembly=HandleObjectComponent
    ComponentClass=VI.JobService.JobComponents.H
andleObjectComponent
    Task=FireGenEvent
    Executiontype=INTERNAL
[Parameters]
    ConnectionProvider=VI.DB.ViSqlFactory,VI.DB
    ConnectionString=Hidden
    EventName=UPDATEUTCOFFSET
    objecttype=DialogTimeZone
    ProclD=9024BED7-58CC-49F2-8CB7-
BF1B443FCA49
    WhereClause=XObjectKey in
('<Key><T>DialogTimeZone</T><P>QBM-
FF60FBBFC1C18061DF4456004FB34D2</P></Key>')
    _paramName1=StopTime
    _paramValue1=2200-01-01 00:00:00.000
2023-03-07 10:51:09 +01:00 - Info: Last process step
request succeeded.
2023-03-07 10:51:09 +01:00 - Info: Loading configuration
parameters...
2023-03-07 10:51:09 +01:00 - Success - \JOBSERVICE01 -
VI.JobService.JobComponents.HandleObjectComponent -
243B18E6-7F33-4784-AEBO-3DE7912D5D55: Successful
    The event UPDATEUTCOFFSET was triggered for 1
object(s) of type DialogTimeZone.
2023-03-07 10:51:24 +01:00 - Info: Requesting process
steps for queue "\JOBSERVICE01".
2023-03-07 10:51:24 +01:00 - Info: Last process step
request succeeded.
2023-03-07 10:51:24 +01:00 - Info: Requesting process
steps for queue "\JOBSERVICE01".
2023-03-07 10:51:24 +01:00 - Parameters - \JOBSERVICE01 -
Process step parameter 3705a023-bea7-4378-8390-
2f9dcb6de695:
    Value=True
2f9dcb6de695:
[Job]
    ComponentAssembly=ScriptComponent
    ComponentClass=VI.JobService.JobComponents.S
criptComponent
    Task=ScriptExec
    Executiontype=EXTERNAL
[Parameters]
    AuthenticationString=Hidden
    ConnectionProvider=VI.DB.ViSqlFactory,VI.DB
    ConnectionString=Hidden
    ProclD=9024BED7-58CC-49F2-8CB7-
BF1B443FCA49
    ScriptName=VID_TimeZone_Update_UTCOFFSet
    StopTime=Hidden
2023-03-07 10:51:24 +01:00 - Info: Last process step
request succeeded.
2023-03-07 10:51:25 +01:00 - Info: Loading configuration
parameters...
2023-03-07 10:51:25 +01:00 - Info: Loading script assembly
WebServices_7bQd6FbE4ufgluWnni6lWFModWoCSv5 from
local cache.
2023-03-07 10:51:25 +01:00 - Info: Loading script assembly
TypedWrappers_7bQd6FbE4ufgluWnni6lWFModWoCSv5 from
local cache.
2023-03-07 10:51:25 +01:00 - Info: Loading script assembly
ProductScripts_7bQd6FbE4ufgluWnni6lWFModWoCSv5 from
local cache.
2023-03-07 10:51:25 +01:00 - Info: Loading script assembly
Scripts_7bQd6FbE4ufgluWnni6lWFModWoCSv5 from local
cache.
2023-03-07 10:51:27 +01:00 - Success - \JOBSERVICE01 -
VI.JobService.JobComponents.ScriptComponent -
3705a023-bea7-4378-8390-2f9dcb6de695: Successful
2023-03-07 10:51:27 +01:00 - Parameters - \JOBSERVICE01 -
Process step output parameter 3705a023-bea7-4378-8390-
2f9dcb6de695:
    Value=True

```

Datensicherung der Arbeit

Die folgenden Screenshots enthalten nicht das ganze Backup-Archiv, sondern lediglich den Stand der Versionierung vom fünften Tag dieser PA.

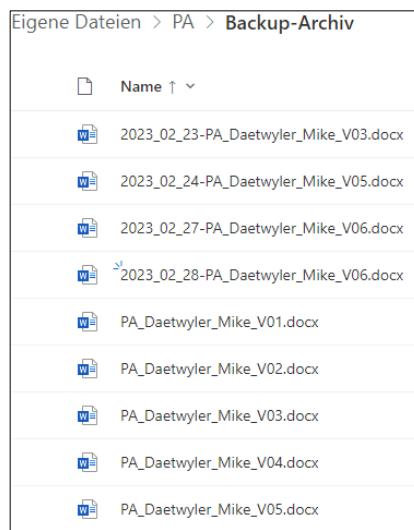


Abbildung 69: Backup-Archiv: OneDrive – Stand vom 01.03.2023 (Dätwyler, 2023)

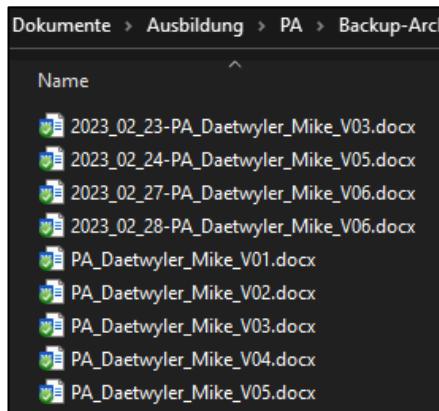


Abbildung 70: Backup-Archiv: Netzlaufwerk – Stand vom 01.03.2023 (Dätwyler, 2023)

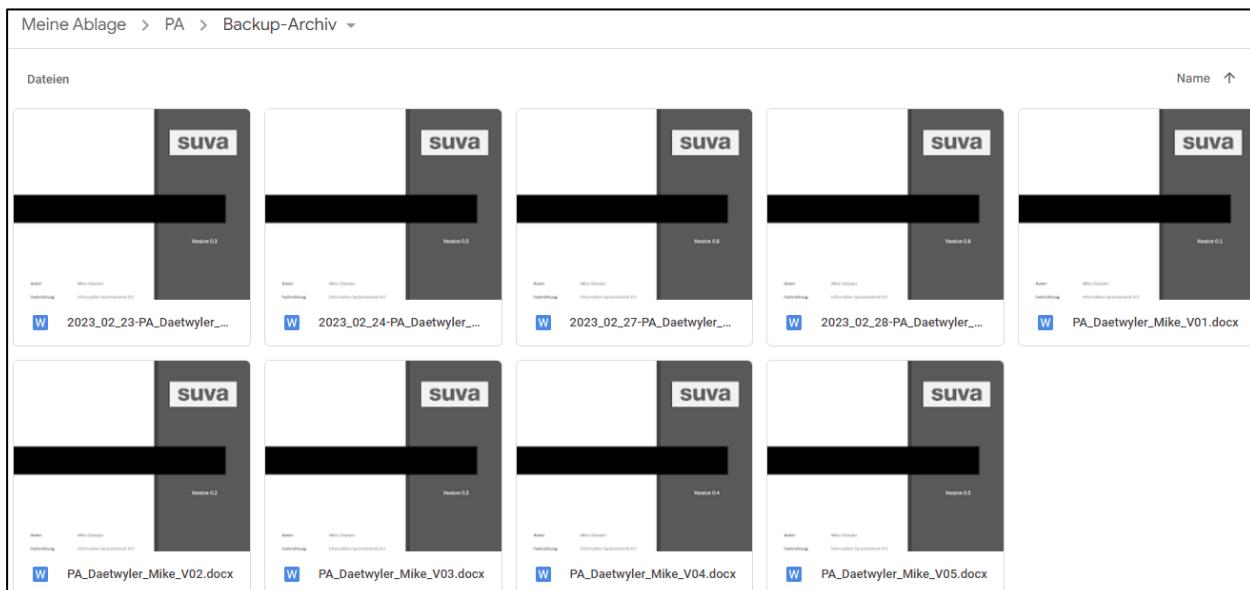


Abbildung 71: Backup-Archiv: Google Drive – Stand vom 01.03.2023 (Dätwyler, 2023)

Jira Software – Scrum Board

The screenshot shows a Jira Scrum Board for the project 'PA' under 'PA board'. The board is titled 'PA Sprint 1' and has three columns: 'TO DO', 'IN PROGRESS', and 'DONE'. The 'TO DO' column contains tasks such as 'Expertenbesuch', 'Identity Manager installieren', 'Identity Manager konfigurieren', 'Installationsanleitung (inkl. Konfiguration) schreiben', 'Mitarbeiter Ex-/Import', 'LDAP System anschliessen', and 'Projektarbeit'. The 'IN PROGRESS' column contains tasks like 'Detailkonzept' and 'Zeitplan erstellen'. The 'DONE' column contains tasks such as 'Einleitung/Ausgangslage', 'Projektbeschreibung', 'Analyse Ist-System', 'Soll-Systembeschreibung', and 'Zeitplan erstellen'. The board also includes filters for 'Epic', 'Bugs', 'Stories', 'Dokumentation Stories', 'Implementation Stories', and 'not solved'. A sidebar on the left provides navigation options for the project.

Column	Task	Progress	Owner
TO DO	Expertenbesuch	0.5	PA
	Identity Manager installieren	2.5	PA
	Identity Manager konfigurieren	2	PA
	Installationsanleitung (inkl. Konfiguration) schreiben	2	PA
	Mitarbeiter Ex-/Import	0.5	PA
	LDAP System anschliessen	0.5	PA
	Projektarbeit	0	PA
IN PROGRESS	Detailkonzept	3.5	PA
	Zeitplan erstellen	1	PA
DONE	Einleitung/Ausgangslage	2	PA
	Projektbeschreibung	1.5	PA
	Analyse Ist-System	1.5	PA
	Soll-Systembeschreibung	1.5	PA
	Zeitplan erstellen	24	MD
	Einleitung/Ausgangslage	25	MD
	Projektbeschreibung	26	MD

Abbildung 72: Scrum Board – Stand vom 27.02.2023 (Dätwyler, 2023)

Epic – Projektarbeit

Projektarbeit

Description
AK:

- Identity Manager installiert und konfiguriert
- Identity Lifecycle implementiert
- Dokumentation verfasst

Child issues

Issue	Status
PA-25 Einleitung/Ausgangslage	DONE
PA-26 Projektbeschreibung	DONE
PA-27 Analyse Ist-System	DONE
PA-28 Soll-Systembeschreibung	DONE

To Do

Details

Story Points: 40

Epic Name: PA

Sprint: PA Sprint 2 +1

Labels: None

Reporter: Mike Dätwyler

Abbildung 73: Epic – Projektarbeit (Dätwyler, 2023)

Story – Tests auswerten

Tests auswerten

Description
AK:

- Testergebnis geschildert
- Testergebnisse ausgewertet
- Ziele ausgewertet

To Do

Details

Story Points: 1

Sprint: PA Sprint 2

Labels: Documentation

Reporter: Mike Dätwyler

Abbildung 74: Story – Tests auswerten (Dätwyler, 2023)

Floatchart

Die Floatcharts vom Kapitel «3.3.4 Identity Lifecycle» und «3.3.5.5 Meine Variante» stützen sich auf die Grundlage des Gelernten aus dem Modul 122. Das Modul 122 besuchte ich in meiner Lehre als Informatik Systemtechnik EFZ im 2. Lehrjahr bei der Lehrperson Erik Benz.

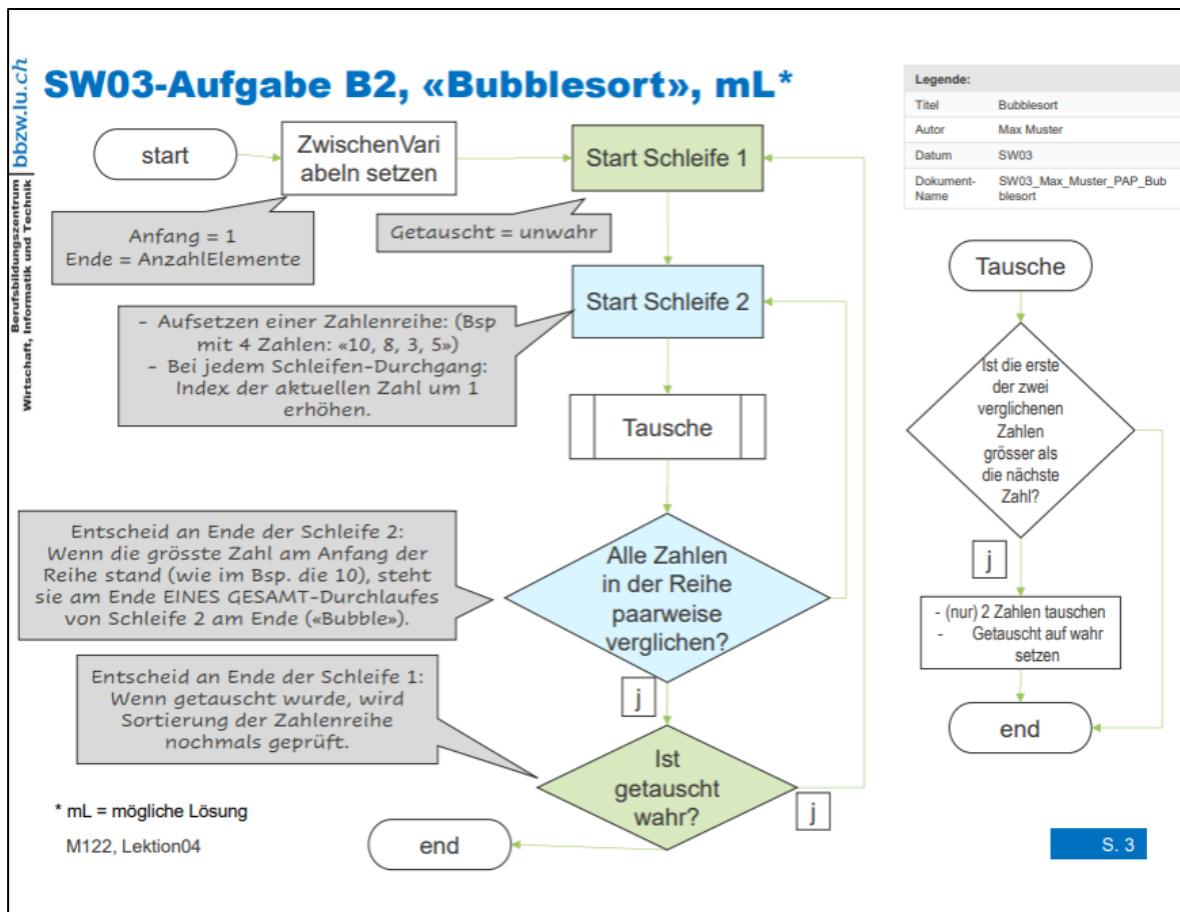


Abbildung 75: Floatchart – Grundlagen (Benz, 2020)

Benutzeranleitung

In der nachfolgenden Inhaltsangabe wird eine Übersicht über die Benutzeranleitung gegeben.

Inhaltsangabe

1	Vorwort	79
1.1	Voraussetzungen	79
1.1.1	Datenbank	79
1.1.2	Identity Manager	79
1.1.3	Identity Lifecycle	79
1.1.4	Kenntnisse	79
2	Vorbereitung	80
2.1	Datenbank	80
2.2	Verbindung auf Server	81
3	Installation	82
3.1	.NET Installation	82
3.2	Identity Manager Installation	83
4	Konfiguration	92
4.1	Job-Service konfigurieren	92
4.2	Config. Parameter konfigurieren	100
4.3	Passwort-Richtlinien und Routine Tasks	106
5	Implementation	109

1 Vorwort

In dieser Anleitung erhalten Sie eine Schritt-für-Schritt-Anleitung zur Installation und Konfiguration des Identity Managers, sowie zur Implementation des Identity Lifecycles mittels «Account Definition mit Geschäftsrolle» auf diesem System.

Für ein detailliertes Verständnis des Identity Lifecycles ist es empfehlenswert, sich die Kapitel «3.3.4 Identity Lifecycle» und «3.3.5.4 Account Definition mit Geschäftsrolle» durchzulesen.

1.1 Voraussetzungen

Für die Installation und Konfiguration, sowie Implementation, wie ich sie durchgeführt habe, müssen gewisse Rahmenbedingungen erfüllt sein. Für das Zusammenragen der technischen Voraussetzungen konnte ich das meiste aus den Release Notes (One Identity, 2023) der Version 9.1 des Identity Managers entnehmen.

1.1.1 Datenbank

- Collation in «SQL_Latin1_General_CI_AS
- Compatability Level auf «150»
- Mindestgrösse nach Suva-Standard ist «16 GB»

1.1.2 Identity Manager

- Microsoft SQL Server 2019
- Microsoft Windows Server 2016
- Microsoft .NET Framework Version 4.8 (oder höher)
- Microsoft Edge WebView2

1.1.3 Identity Lifecycle

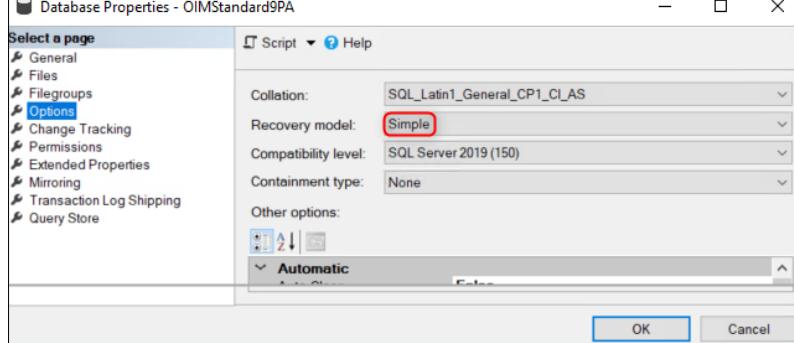
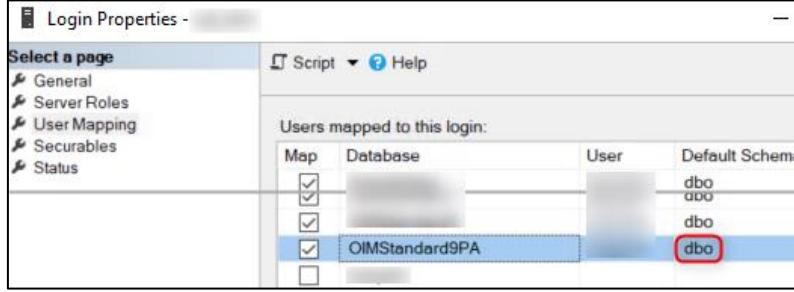
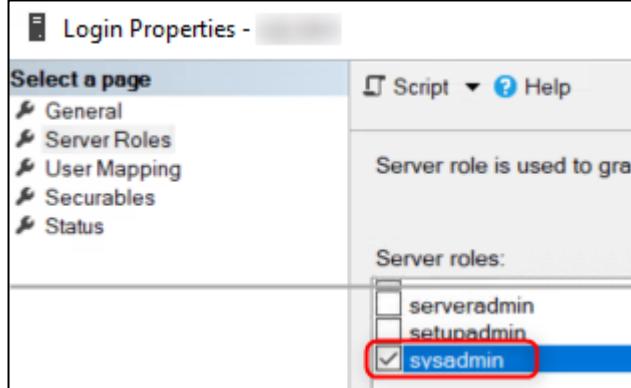
- Identity Manager in der Version 9.1 von One Identity
 - Anbindung eins LDAP-Verzeichnisses

1.1.4 Kenntnisse

- IT-Affinität
- SQL-Basiswissen (Falls ein eigener Filter erstellt werden möchte)
- Identity & Access Management Grundwissen von Vorteil

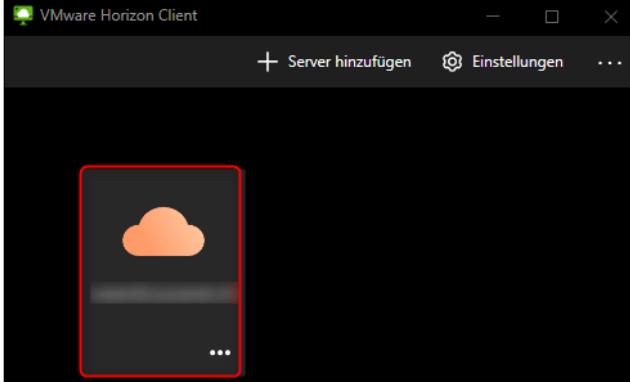
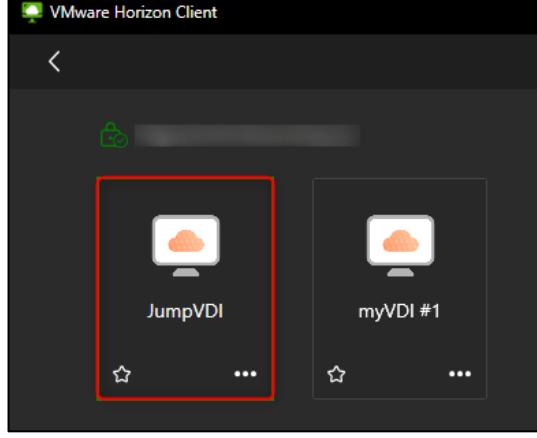
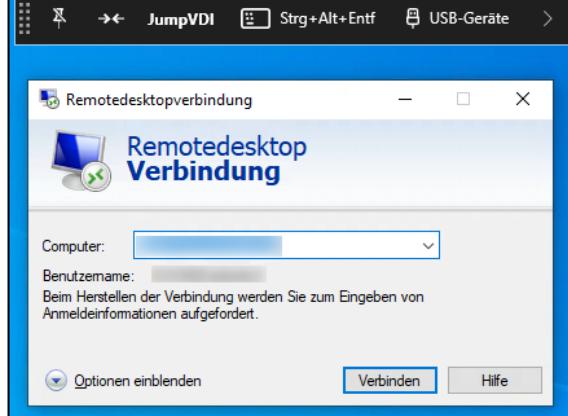
2 Vorbereitung

2.1 Datenbank

Schritt	Visuelle Darstellung
Vor der Installation ist es wichtig, dass man bei der verwendeten IAM-Datenbank das Recovery model auf «Simple» stellt.	
Der verwendete SQL-Admin-User muss zudem noch «Database owner» auf der IAM-Datenbank sein.	
Der SQL-Admin-User ebenfalls die Rolle «sysadmin» erhalten.	

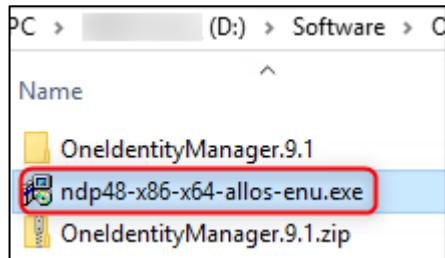
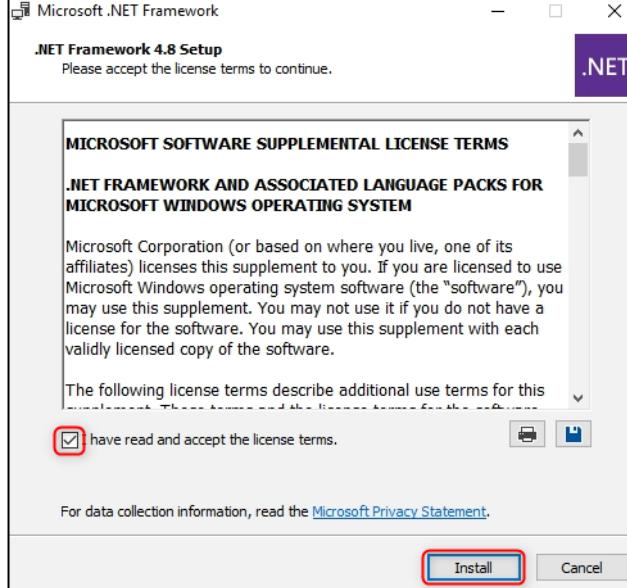
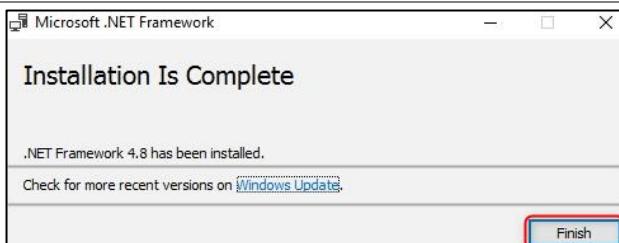
2.2 Verbindung auf Server

Bevor man das IAM-System überhaupt installieren kann, muss man sich natürlich erst auf den Server verbinden, auf welchem das IAM-System installiert werden soll. Den entsprechenden Vorgang dazu habe ich bereits im Kapitel «3.2.1.4 Serverumgebung» erläutert, ist aber trotzdem nochmals, unten abgebildet.

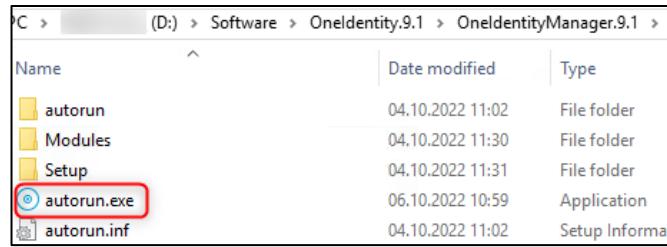
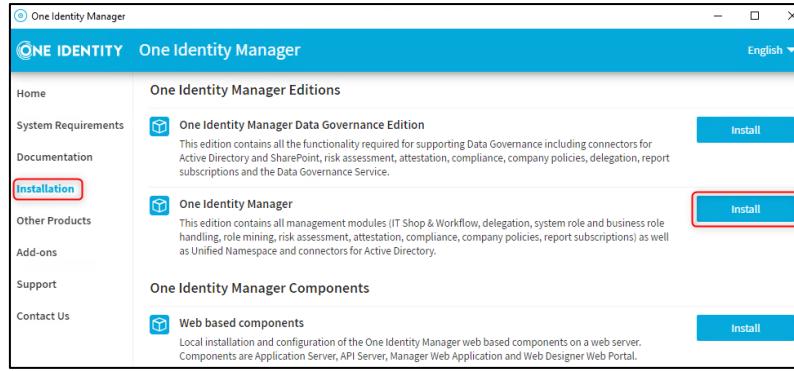
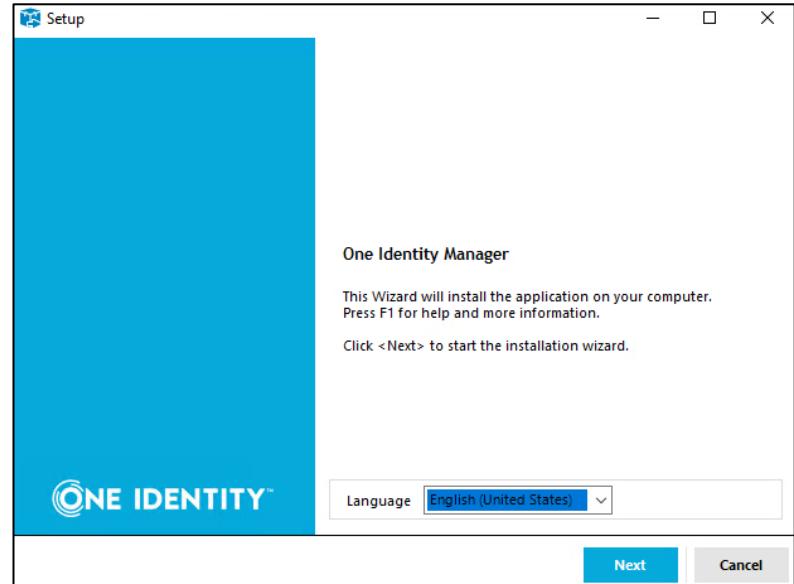
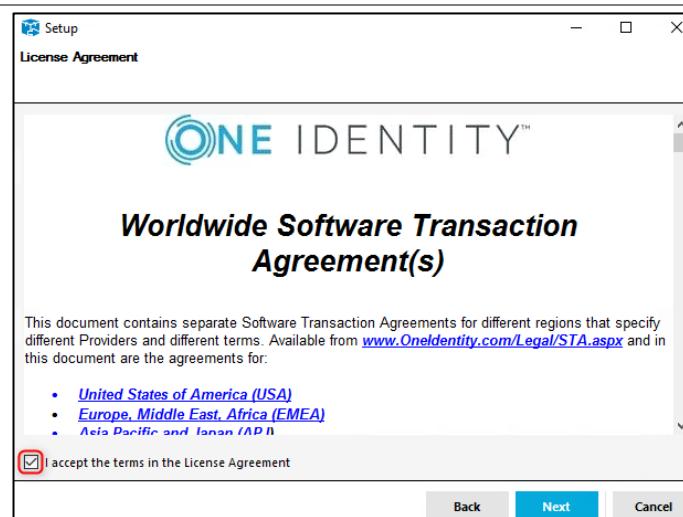
Schritt	Visuelle Darstellung
Als erstes muss man den <u>VMware Horizon Client</u> starten.	
Wenn man sich mit dem eigenen Login eingewählt hat, kann man VDIs sehen, zu welchen man Zugriff hat. Dabei sollte sich die JumpVDI befinden, welche man dann auch wählen muss.	
In der VDI angekommen, verbindet man sich nun per RDP auf den Server, auf welchem man das IAM-System installieren möchte.	

3 Installation

3.1 .NET Installation

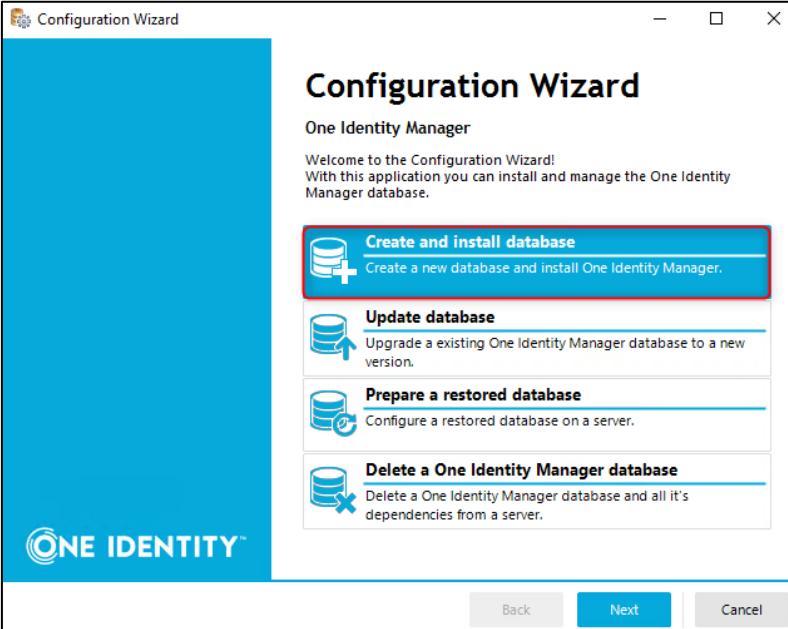
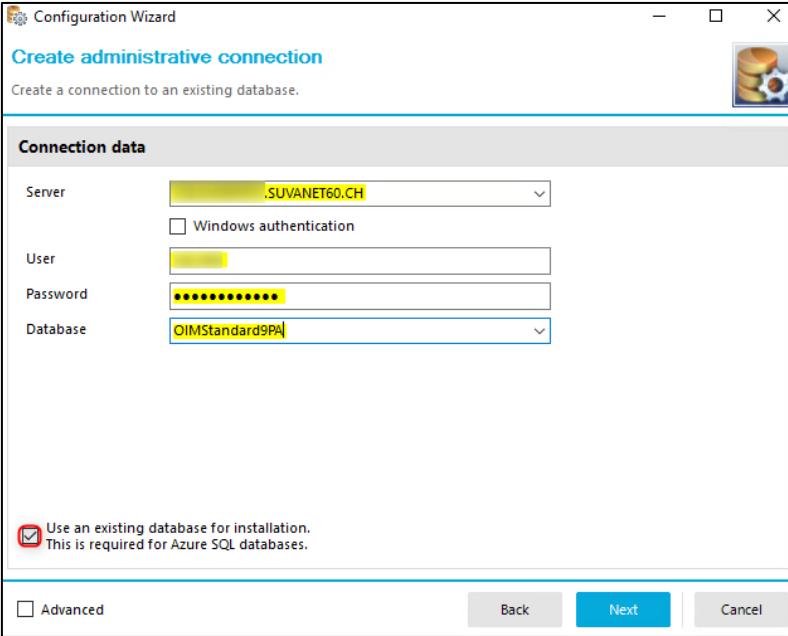
Schritt	Visuelle Darstellung
Die .exe-Datei von .NET 4.8 ausführen.	
Lizenzierungsbedingungen akzeptieren und auf «Install» klicken.	
.NET 4.8 ist nun beinahe installiert. Es fehlt nur noch ein Neustart des Servers. Hierbei muss abgeklärt werden, ob der Server einfach so neugestartet werden darf.	
Nach dem Neustart kann es einen Moment dauern bis .NET voll funktionsfähig ist, weshalb es sich empfiehlt nach dem Neustart noch ca. 5 Minuten mit der Installation des Identity Managers zu warten.	

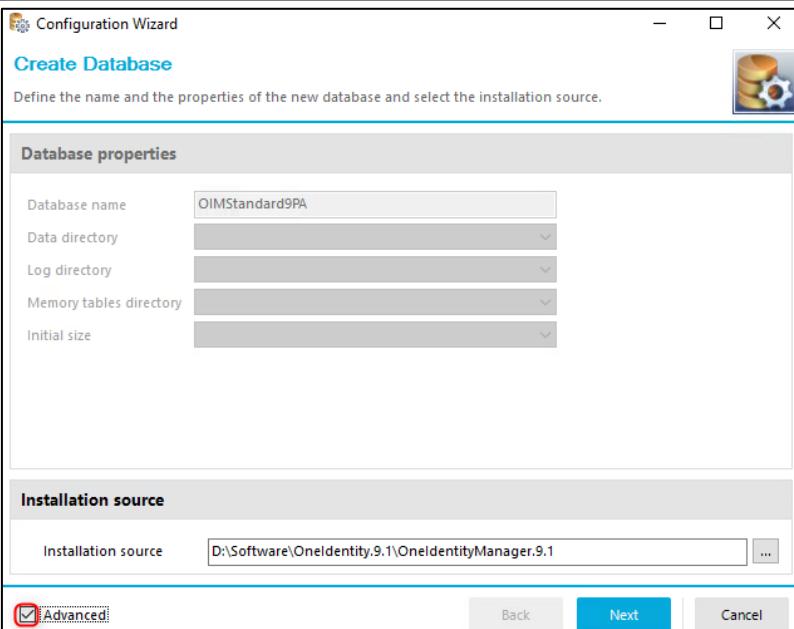
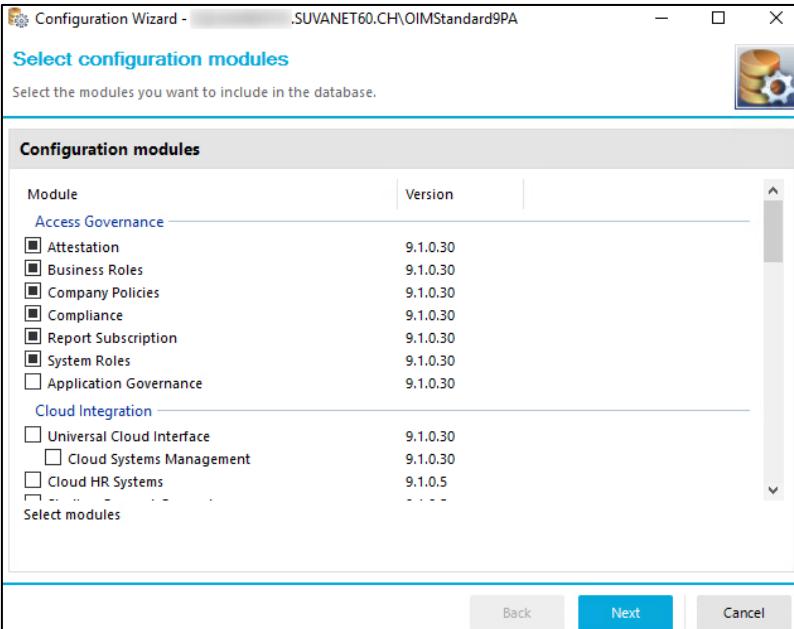
3.2 Identity Manager Installation

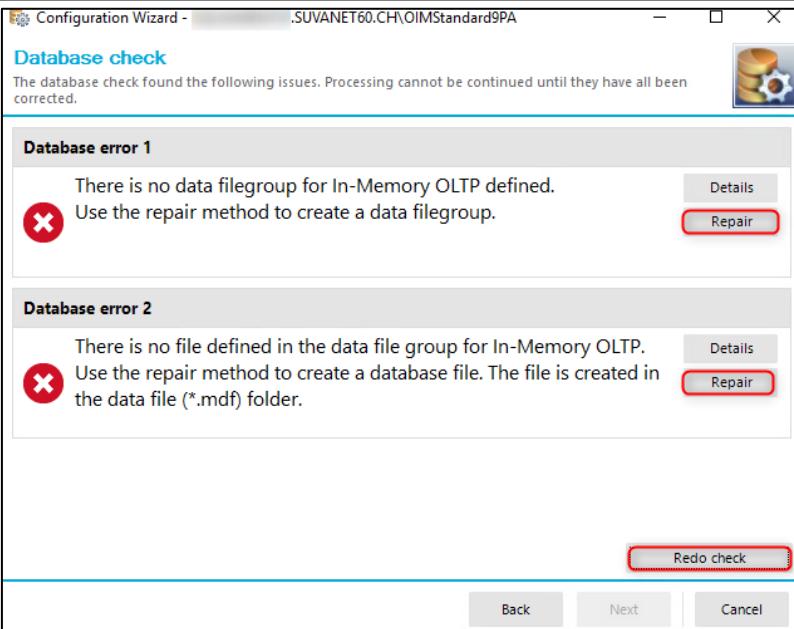
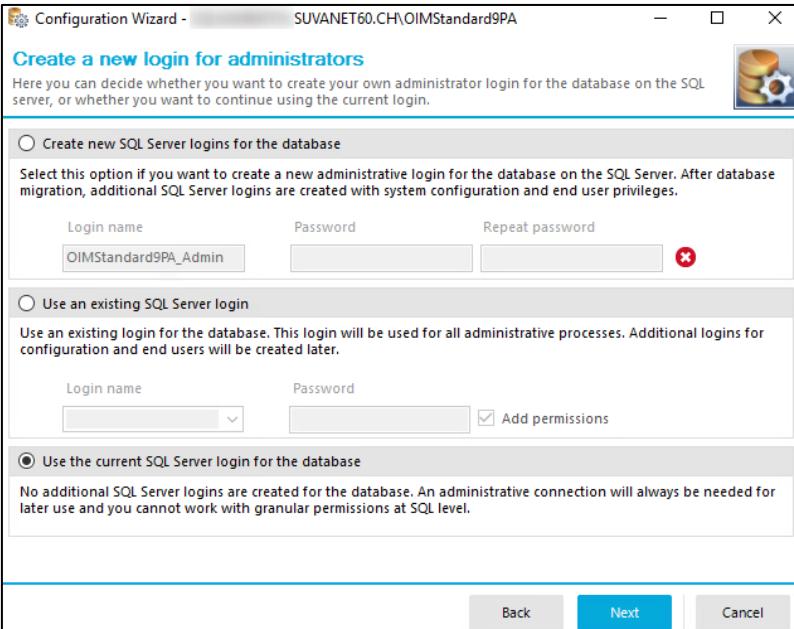
Schritt	Visuelle Darstellung
Die .exe des Setups für den Identity Manager ausführen.	
Im Setup muss man dann zum Kapitel «Installation» gehen und den «One Identity Manager» wählen.	
Installiert wird der Identity Manager auf Englisch, nach Suva-Standard.	
Lizenzierungsbedingungen akzeptieren und auf «Next» klicken.	

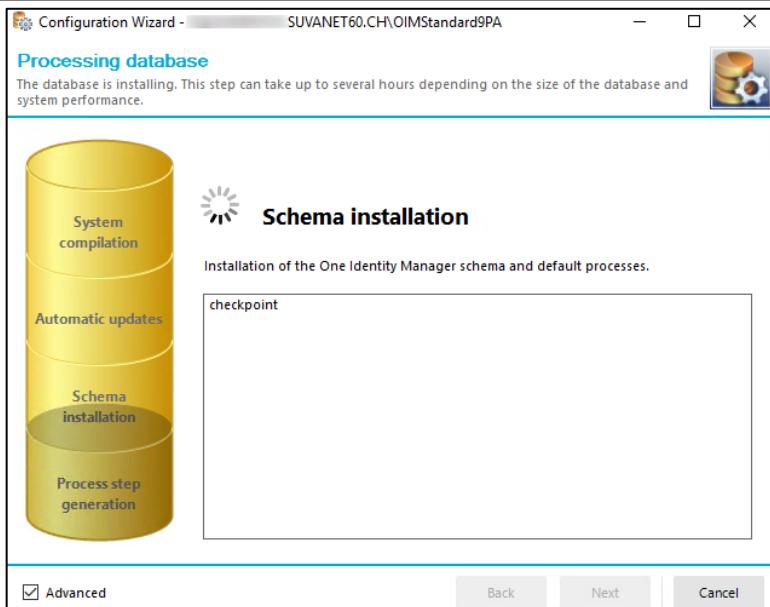
<p>Bei diesem Fenster wählt man das Installationsverzeichnis und wählt aus, dass man zusätzliche Module installieren möchte.</p>																																																																													
<p>Hier werden folgende Module gewählt:</p> <ul style="list-style-type: none"> - Microsoft Exchange - LDAP directories - SAP R/3 	<table border="1"> <thead> <tr> <th>All</th> <th>None</th> <th>Module</th> <th>Version</th> </tr> </thead> <tbody> <tr><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>Target Systems</td><td></td></tr> <tr><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td><td>Active Directory</td><td>9.1.0.30</td></tr> <tr><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td><td>Microsoft Exchange</td><td>9.1.0.30</td></tr> <tr><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>Exchange hybrid</td><td>9.1.0.30</td></tr> <tr><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>SharePoint</td><td>9.1.0.30</td></tr> <tr><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>Azure Active Directory</td><td>9.1.0.30</td></tr> <tr><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>Exchange Online</td><td>9.1.0.30</td></tr> <tr><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>Microsoft Teams</td><td>9.1.0.30</td></tr> <tr><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>SharePoint Online</td><td>9.1.0.30</td></tr> <tr><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>Google Workspace</td><td>9.1.0.30</td></tr> <tr><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>Domino</td><td>9.1.0.30</td></tr> <tr><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td><td>LDAP directories</td><td>9.1.0.30</td></tr> <tr><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>Mainframe</td><td>9.1.0.30</td></tr> <tr><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>Oracle E-Business Suite</td><td>9.1.0.30</td></tr> <tr><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>Privileged Account Governance</td><td>9.1.0.30</td></tr> <tr><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td><td>SAP R/3</td><td>9.1.0.30</td></tr> <tr><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>SAP R/3 Structural Profiles Add-on</td><td>9.1.0.30</td></tr> <tr><td colspan="4">Base Technology</td></tr> </tbody> </table>	All	None	Module	Version	<input type="checkbox"/>	<input type="checkbox"/>	Target Systems		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Active Directory	9.1.0.30	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Microsoft Exchange	9.1.0.30	<input type="checkbox"/>	<input type="checkbox"/>	Exchange hybrid	9.1.0.30	<input type="checkbox"/>	<input type="checkbox"/>	SharePoint	9.1.0.30	<input type="checkbox"/>	<input type="checkbox"/>	Azure Active Directory	9.1.0.30	<input type="checkbox"/>	<input type="checkbox"/>	Exchange Online	9.1.0.30	<input type="checkbox"/>	<input type="checkbox"/>	Microsoft Teams	9.1.0.30	<input type="checkbox"/>	<input type="checkbox"/>	SharePoint Online	9.1.0.30	<input type="checkbox"/>	<input type="checkbox"/>	Google Workspace	9.1.0.30	<input type="checkbox"/>	<input type="checkbox"/>	Domino	9.1.0.30	<input checked="" type="checkbox"/>	<input type="checkbox"/>	LDAP directories	9.1.0.30	<input type="checkbox"/>	<input type="checkbox"/>	Mainframe	9.1.0.30	<input type="checkbox"/>	<input type="checkbox"/>	Oracle E-Business Suite	9.1.0.30	<input type="checkbox"/>	<input type="checkbox"/>	Privileged Account Governance	9.1.0.30	<input checked="" type="checkbox"/>	<input type="checkbox"/>	SAP R/3	9.1.0.30	<input type="checkbox"/>	<input type="checkbox"/>	SAP R/3 Structural Profiles Add-on	9.1.0.30	Base Technology			
All	None	Module	Version																																																																										
<input type="checkbox"/>	<input type="checkbox"/>	Target Systems																																																																											
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Active Directory	9.1.0.30																																																																										
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Microsoft Exchange	9.1.0.30																																																																										
<input type="checkbox"/>	<input type="checkbox"/>	Exchange hybrid	9.1.0.30																																																																										
<input type="checkbox"/>	<input type="checkbox"/>	SharePoint	9.1.0.30																																																																										
<input type="checkbox"/>	<input type="checkbox"/>	Azure Active Directory	9.1.0.30																																																																										
<input type="checkbox"/>	<input type="checkbox"/>	Exchange Online	9.1.0.30																																																																										
<input type="checkbox"/>	<input type="checkbox"/>	Microsoft Teams	9.1.0.30																																																																										
<input type="checkbox"/>	<input type="checkbox"/>	SharePoint Online	9.1.0.30																																																																										
<input type="checkbox"/>	<input type="checkbox"/>	Google Workspace	9.1.0.30																																																																										
<input type="checkbox"/>	<input type="checkbox"/>	Domino	9.1.0.30																																																																										
<input checked="" type="checkbox"/>	<input type="checkbox"/>	LDAP directories	9.1.0.30																																																																										
<input type="checkbox"/>	<input type="checkbox"/>	Mainframe	9.1.0.30																																																																										
<input type="checkbox"/>	<input type="checkbox"/>	Oracle E-Business Suite	9.1.0.30																																																																										
<input type="checkbox"/>	<input type="checkbox"/>	Privileged Account Governance	9.1.0.30																																																																										
<input checked="" type="checkbox"/>	<input type="checkbox"/>	SAP R/3	9.1.0.30																																																																										
<input type="checkbox"/>	<input type="checkbox"/>	SAP R/3 Structural Profiles Add-on	9.1.0.30																																																																										
Base Technology																																																																													
<p>Als Nächstes werden alle «Machine roles» ausgewählt.</p>																																																																													

<p>Jetzt erstellt man einen Job-Service, welcher auf dem Server installiert wird, auf welchem das Setup ausgeführt wird. (also auf dem Server, auf welchem das IAM laufen wird)</p>	
<p>Den «Configuration Wizard» starten.</p>	

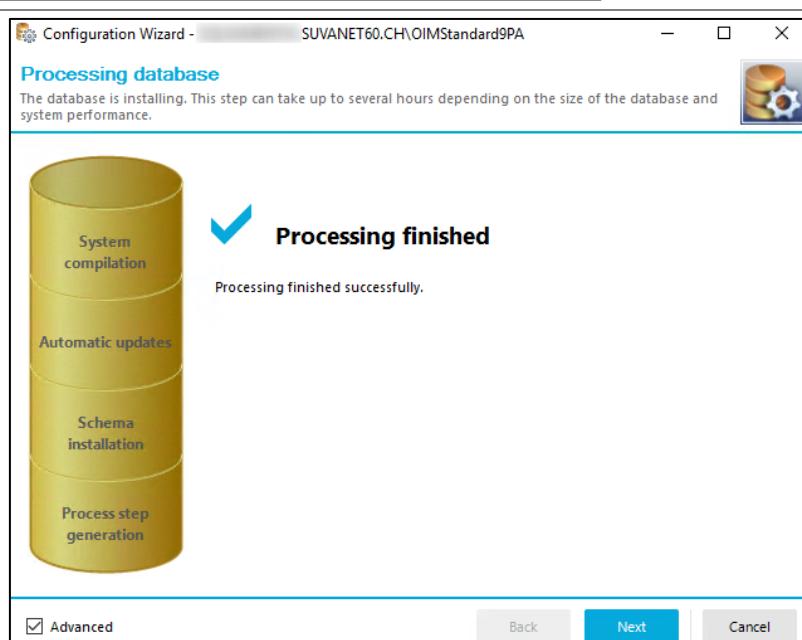
<p>Hier «Create and install database» wählen.</p>	 <p>Configuration Wizard One Identity Manager Welcome to the Configuration Wizard! With this application you can install and manage the One Identity Manager database.</p> <ul style="list-style-type: none"> Create and install database Create a new database and install One Identity Manager. Update database Upgrade a existing One Identity Manager database to a new version. Prepare a restored database Configure a restored database on a server. Delete a One Identity Manager database Delete a One Identity Manager database and all it's dependencies from a server. <p>Back Next Cancel</p>								
<p>Verbinden auf den SQL-Server, per SQL-Admin-User, auf welchem die DB läuft. Hier wählen, dass man eine bereits existierende DB verwenden möchte.</p>	 <p>Create administrative connection Create a connection to an existing database.</p> <p>Connection data</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 2px;">Server</td> <td style="padding: 2px;"><input type="text" value=".SUVANET60.CH"/></td> </tr> <tr> <td style="padding: 2px;">User</td> <td style="padding: 2px;"><input type="text"/></td> </tr> <tr> <td style="padding: 2px;">Password</td> <td style="padding: 2px;"><input type="password" value="*****"/></td> </tr> <tr> <td style="padding: 2px;">Database</td> <td style="padding: 2px;"><input type="text" value="OIMStandard9P%"/></td> </tr> </table> <p><input checked="" type="checkbox"/> Use an existing database for installation. This is required for Azure SQL databases.</p> <p><input type="checkbox"/> Advanced Back Next Cancel</p>	Server	<input type="text" value=".SUVANET60.CH"/>	User	<input type="text"/>	Password	<input type="password" value="*****"/>	Database	<input type="text" value="OIMStandard9P%"/>
Server	<input type="text" value=".SUVANET60.CH"/>								
User	<input type="text"/>								
Password	<input type="password" value="*****"/>								
Database	<input type="text" value="OIMStandard9P%"/>								

Hier die Quelle der Installation vom Identity Manager angeben.	
Bei diesem Schritt können nochmals die zu installierenden Module überprüft werden.	

<p>Wenn diese Fehler auftauchen, liegt ein Problem auf der Datenbank vor. Mit «repair» können diese einfach gelöst werden. Wenn nach einem «Redo check» kein Fehler mehr vorhanden ist, kann man zum nächsten Punkt gelangen.</p>	 <p>The screenshot shows the 'Database check' step of the Configuration Wizard. It displays two errors:</p> <ul style="list-style-type: none"> Database error 1: There is no data filegroup for In-Memory OLTP defined. Repair button highlighted. Database error 2: There is no file defined in the data file group for In-Memory OLTP. Repair button highlighted. <p>At the bottom right of the window, the Redo check button is also highlighted with a red box.</p>
<p>Hier wird der vorher angegebene SQL-Admin-User verwendet, nach Suva-Standard.</p>	 <p>The screenshot shows the 'Create a new login for administrators' step of the Configuration Wizard. It offers three options:</p> <ul style="list-style-type: none"> <input type="radio"/> Create new SQL Server logins for the database <input type="radio"/> Use an existing SQL Server login <input checked="" type="radio"/> Use the current SQL Server login for the database <p>The third option is selected and highlighted with a red box. The 'Add permissions' checkbox is checked.</p>

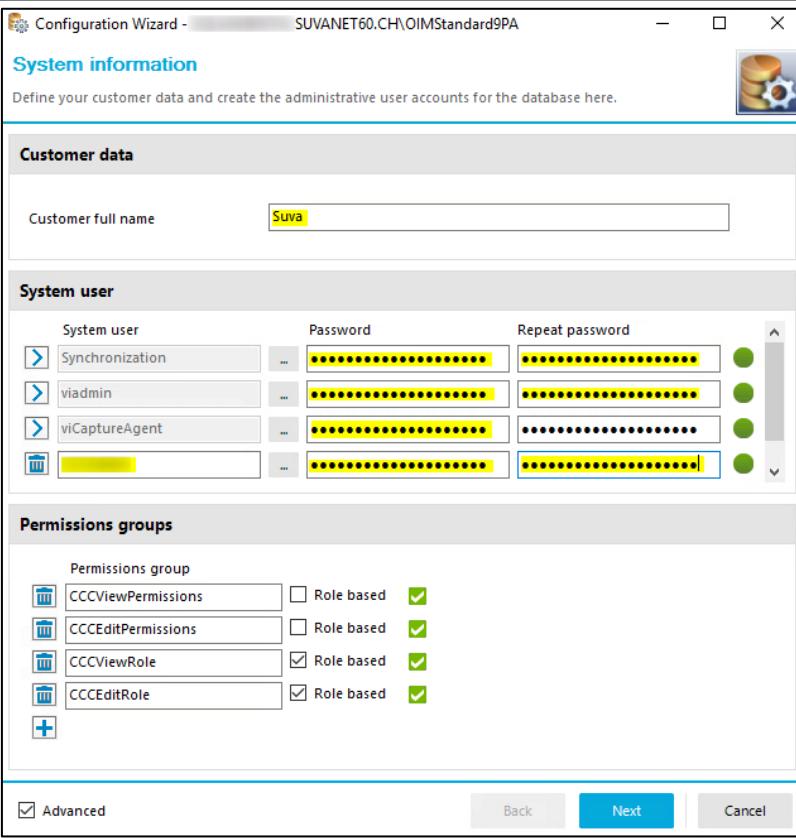
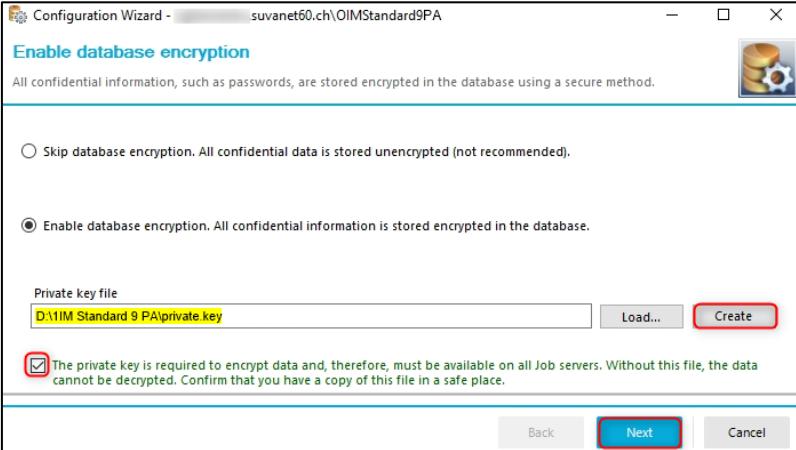
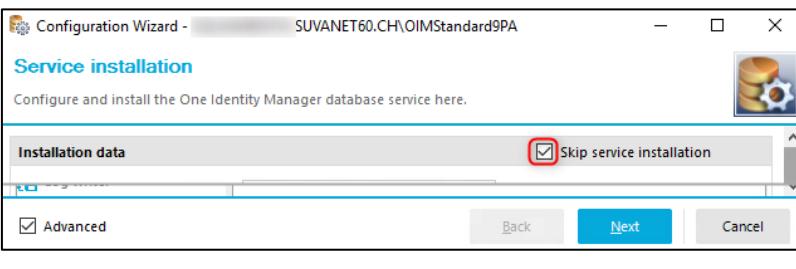


The screenshot shows the 'Processing database' step of the Configuration Wizard. The title bar reads 'Configuration Wizard - SUVANET60.CH\OIMStandard9PA'. The main content area is titled 'Schema installation' with the sub-instruction 'Installation of the One Identity Manager schema and default processes.' A large yellow cylinder icon on the left is divided into four sections: 'System compilation' (top), 'Automatic updates' (second), 'Schema installation' (third), and 'Process step generation' (bottom). To the right of the cylinder, there is a 'checkpoint' box which is currently empty. At the bottom of the window are buttons for 'Back', 'Next', and 'Cancel', with an 'Advanced' checkbox checked.



The screenshot shows the 'Processing database' step of the Configuration Wizard after completion. The title bar remains the same. The main content area is titled 'Processing finished' with the sub-instruction 'Processing finished successfully.' A large yellow cylinder icon is shown, identical to the one in the previous screenshot. A blue checkmark icon is positioned to the left of the cylinder. At the bottom of the window are buttons for 'Back', 'Next', and 'Cancel', with an 'Advanced' checkbox checked.

Wenn die Datenbank installiert ist, auf «Next» klicken.

<p>In der Suva erstellen wir jeweils einen eigenen User, welcher Berechtigungen analog dem «viadmin» besitzt. Dieser wird nun hier angelegt.</p>	
<p>Um die DB verschlüsseln zu können, muss ein private.key-File erstellt werden.</p> <p>Wichtig: Unbedingt ein Backup der Datei machen und es an einem anderen Ort als das Installationsverzeichnis abspeichern, da das Original aus Sicherheitsgründen aus dem Installationsverzeichnis gelöscht wird.</p>	
<p>Dieser Schritt muss übersprungen werden, da man hierbei einen Job-Service installieren würde. Die Hoheit über den SQL-Server haben aber nicht wir, sondern der DBA. Zudem hat es bereits einen Job-Service auf dem Server, auf welchem das IAM installiert wird.</p>	

<p>Nun kann man die Installation beenden.</p>	<p>Configuration Wizard finished</p> <p>You have successfully completed the wizard.</p> <ul style="list-style-type: none"> Launchpad Start the central administration tool. Run Manager Manage employees, user accounts and target systems. Run Designer Configure the system. Run <p>ONE IDENTITY™</p> <p>Finish</p>
<p>Da die Installation nun beendet ist, muss das Recovery model der IAM-Datenbank wieder auf «Full» gestellt werden.</p>	<p>Database Properties - OIMStandard9PA</p> <p>Select a page</p> <ul style="list-style-type: none"> General Files Filegroups Options Change Tracking Permissions Extended Properties Mirroring Transaction Log Shipping Query Store <p>Collation: SQL_Latin1_General_CI_AS</p> <p>Recovery model: Full</p> <p>Compatibility level: SQL Server 2019 (150)</p> <p>Containment type: None</p> <p>Other options:</p> <p>Automatic Auto Close False</p> <p>OK</p>
<p>Dem verwendeten SQL-Admin-User sollte die «sysadmin»-Berechtigung wieder entzogen werden.</p>	<p>Login Properties -</p> <p>Select a page</p> <ul style="list-style-type: none"> General Server Roles User Mapping Securables Status <p>Server roles:</p> <ul style="list-style-type: none"> bulkadmin serveradmin setupadmin sysadmin

4 Konfiguration

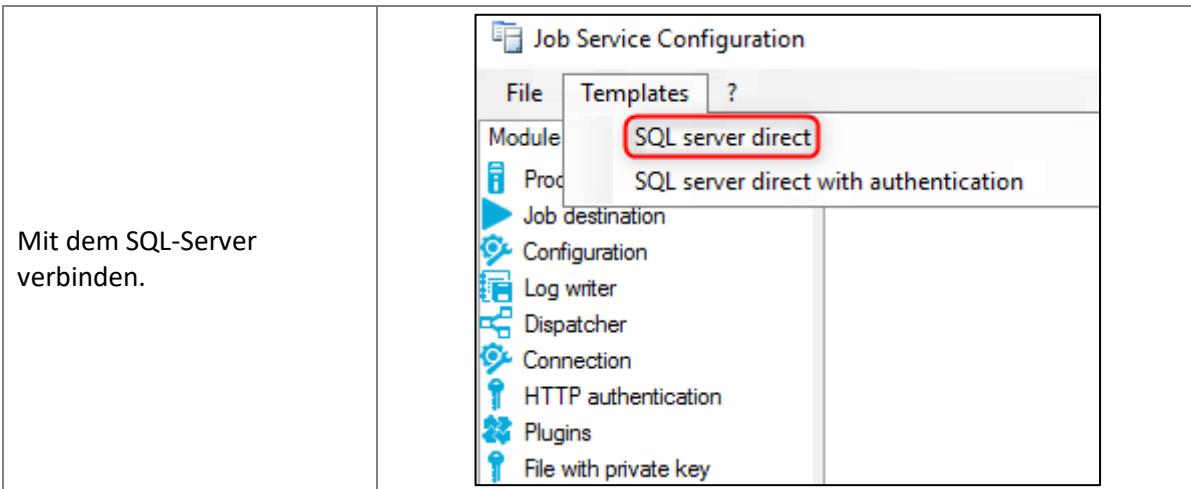
Nach der erfolgreichen Installation des Identity Managers, muss dieser nun noch ein bisschen konfiguriert werden, damit er dem Suva-Standard gerecht wird.

4.1 Job-Service konfigurieren

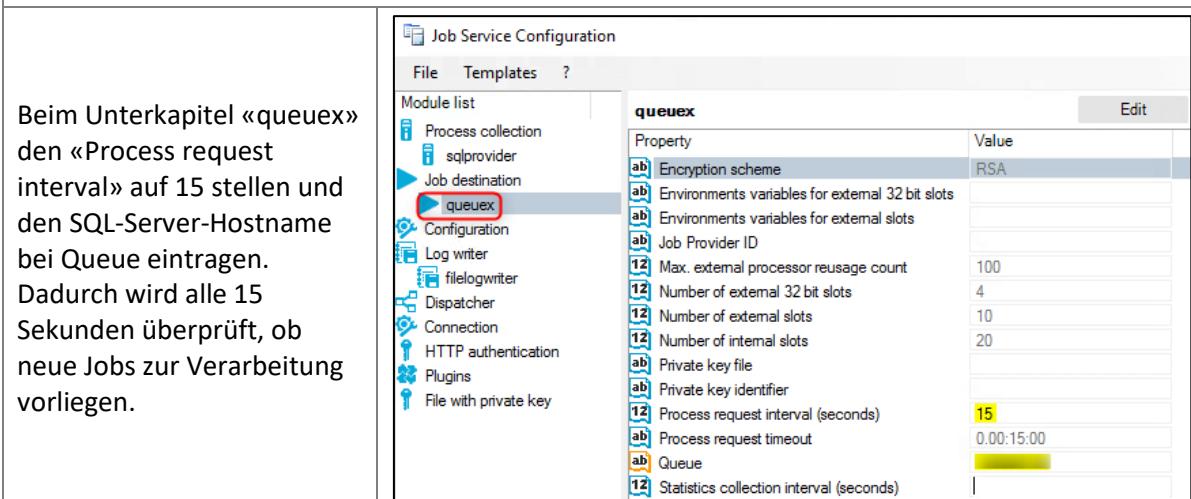
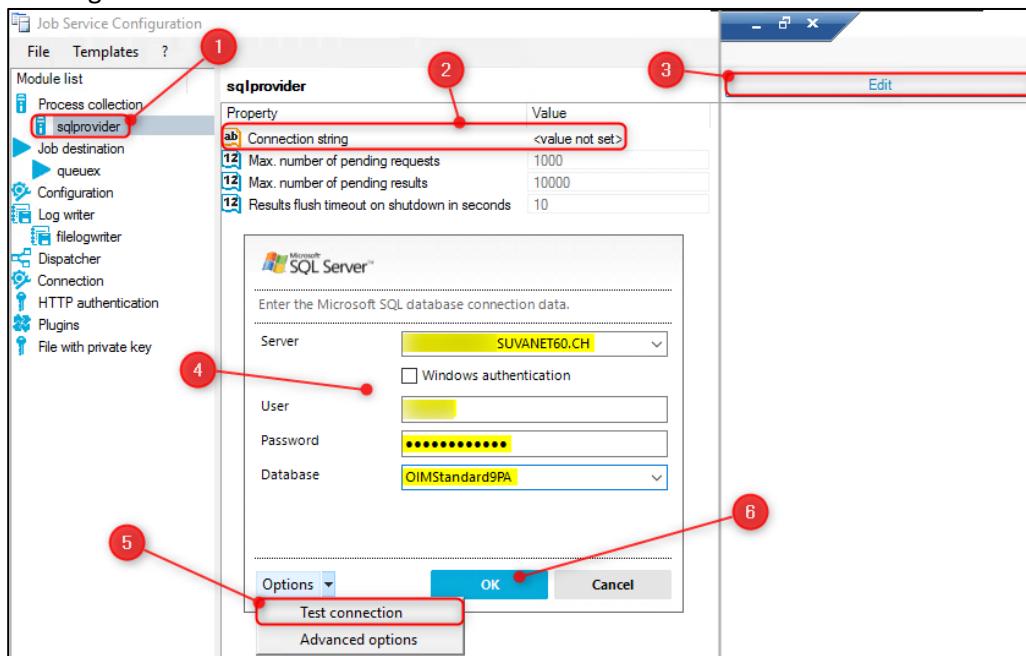
Schritt	Visuelle Darstellung
Den Designer über das Launchpad öffnen.	
Unter «Add Job server» den eingetragenen Job-Server wie folgt anpassen:	
Server [Hostname]	SQL-Server
Executing Server [FQDN]	Server, auf welchem das IAM läuft
Queue [Hostname]	\SQL-Server
Full server name [FQDN]	Server, auf welchem das IAM läuft
Danach zum Kapitel «Network» wechseln und folgendes anpasse:	

<p>Als Nächstes die Kategorie unten zu «Server function» wechseln und die abgebildeten Häkchen setzen.</p>	<table border="1"> <thead> <tr> <th>Server function</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> SQL processing server</td> <td>Server is able to run SQL tasks.</td> </tr> <tr> <td><input checked="" type="checkbox"/> Update server</td> <td>Server handles automatic software ...</td> </tr> <tr> <td><input type="checkbox"/> Active Directory connector</td> <td>Server is able to connect to Active ...</td> </tr> <tr> <td><input type="checkbox"/> Active Roles connector</td> <td>Server is able to connect to Active ...</td> </tr> <tr> <td><input checked="" type="checkbox"/> CSV connector</td> <td>Server can process CSV files. (CSV c...</td> </tr> <tr> <td><input type="checkbox"/> File script server</td> <td>Home directories for user accounts...</td> </tr> <tr> <td><input checked="" type="checkbox"/> LDAP connector</td> <td>Server is able to connect to LDAP. (...</td> </tr> <tr> <td><input type="checkbox"/> SCIM connector</td> <td>The server can connect to a cloud a...</td> </tr> <tr> <td><input checked="" type="checkbox"/> SMTP host</td> <td>Server is able to send emails.</td> </tr> <tr> <td><input type="checkbox"/> Windows PowerShell Connector</td> <td>Server is able to run Windows Pow...</td> </tr> </tbody> </table>	Server function	Description	<input checked="" type="checkbox"/> SQL processing server	Server is able to run SQL tasks.	<input checked="" type="checkbox"/> Update server	Server handles automatic software ...	<input type="checkbox"/> Active Directory connector	Server is able to connect to Active ...	<input type="checkbox"/> Active Roles connector	Server is able to connect to Active ...	<input checked="" type="checkbox"/> CSV connector	Server can process CSV files. (CSV c...	<input type="checkbox"/> File script server	Home directories for user accounts...	<input checked="" type="checkbox"/> LDAP connector	Server is able to connect to LDAP. (...	<input type="checkbox"/> SCIM connector	The server can connect to a cloud a...	<input checked="" type="checkbox"/> SMTP host	Server is able to send emails.	<input type="checkbox"/> Windows PowerShell Connector	Server is able to run Windows Pow...
Server function	Description																						
<input checked="" type="checkbox"/> SQL processing server	Server is able to run SQL tasks.																						
<input checked="" type="checkbox"/> Update server	Server handles automatic software ...																						
<input type="checkbox"/> Active Directory connector	Server is able to connect to Active ...																						
<input type="checkbox"/> Active Roles connector	Server is able to connect to Active ...																						
<input checked="" type="checkbox"/> CSV connector	Server can process CSV files. (CSV c...																						
<input type="checkbox"/> File script server	Home directories for user accounts...																						
<input checked="" type="checkbox"/> LDAP connector	Server is able to connect to LDAP. (...																						
<input type="checkbox"/> SCIM connector	The server can connect to a cloud a...																						
<input checked="" type="checkbox"/> SMTP host	Server is able to send emails.																						
<input type="checkbox"/> Windows PowerShell Connector	Server is able to run Windows Pow...																						
<p>Dann die Kategorie nochmals wechseln, dieses Mal zu «Machine role». Hierbei müssen alle Rollen ausgewählt werden, da es nur einen Job-Server gibt.</p>	<table border="1"> <thead> <tr> <th>Machine role</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> Database Agent</td> </tr> <tr> <td><input checked="" type="checkbox"/> Documentation</td> </tr> <tr> <td><input checked="" type="checkbox"/> HTML Development</td> </tr> <tr> <td><input type="checkbox"/> Server</td> </tr> <tr> <td><input checked="" type="checkbox"/> Job Server</td> </tr> <tr> <td><input checked="" type="checkbox"/> Active Directory</td> </tr> <tr> <td><input checked="" type="checkbox"/> Microsoft Exchange</td> </tr> <tr> <td><input checked="" type="checkbox"/> Configuration tool</td> </tr> <tr> <td><input checked="" type="checkbox"/> LDAP directories</td> </tr> <tr> <td><input checked="" type="checkbox"/> SAP R/3</td> </tr> <tr> <td><input checked="" type="checkbox"/> SCIM</td> </tr> <tr> <td><input type="checkbox"/> Workstation</td> </tr> <tr> <td><input checked="" type="checkbox"/> Administration</td> </tr> <tr> <td><input checked="" type="checkbox"/> CommandlineAdministration</td> </tr> <tr> <td><input checked="" type="checkbox"/> Configuration</td> </tr> <tr> <td><input checked="" type="checkbox"/> Development and Testing</td> </tr> <tr> <td><input checked="" type="checkbox"/> Monitoring</td> </tr> </tbody> </table>	Machine role	<input checked="" type="checkbox"/> Database Agent	<input checked="" type="checkbox"/> Documentation	<input checked="" type="checkbox"/> HTML Development	<input type="checkbox"/> Server	<input checked="" type="checkbox"/> Job Server	<input checked="" type="checkbox"/> Active Directory	<input checked="" type="checkbox"/> Microsoft Exchange	<input checked="" type="checkbox"/> Configuration tool	<input checked="" type="checkbox"/> LDAP directories	<input checked="" type="checkbox"/> SAP R/3	<input checked="" type="checkbox"/> SCIM	<input type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Administration	<input checked="" type="checkbox"/> CommandlineAdministration	<input checked="" type="checkbox"/> Configuration	<input checked="" type="checkbox"/> Development and Testing	<input checked="" type="checkbox"/> Monitoring				
Machine role																							
<input checked="" type="checkbox"/> Database Agent																							
<input checked="" type="checkbox"/> Documentation																							
<input checked="" type="checkbox"/> HTML Development																							
<input type="checkbox"/> Server																							
<input checked="" type="checkbox"/> Job Server																							
<input checked="" type="checkbox"/> Active Directory																							
<input checked="" type="checkbox"/> Microsoft Exchange																							
<input checked="" type="checkbox"/> Configuration tool																							
<input checked="" type="checkbox"/> LDAP directories																							
<input checked="" type="checkbox"/> SAP R/3																							
<input checked="" type="checkbox"/> SCIM																							
<input type="checkbox"/> Workstation																							
<input checked="" type="checkbox"/> Administration																							
<input checked="" type="checkbox"/> CommandlineAdministration																							
<input checked="" type="checkbox"/> Configuration																							
<input checked="" type="checkbox"/> Development and Testing																							
<input checked="" type="checkbox"/> Monitoring																							
<p>Jetzt müssen die Änderungen noch auf der Datenbank gespeichert werden, indem man hier noch einen «Commit to database» ausführt.</p>	<p>Designer - .SUUVANETI</p> <p>Database Job Server View Help</p> <p>Commit to database Back Next ?</p> <p>Navigation</p> <p>Getting Started</p> <p>Create administrator</p> <p>Save changed objects to the database.</p> <p>All changed objects, grouped by editor are displayed in the list. Click 'Save' to save changes to main database.</p> <p>Change label <no change label></p> <table border="1"> <thead> <tr> <th>Editor / Object</th> <th>Old value</th> <th>New value</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> </tr> </tbody> </table> <p>Save Cancel</p>	Editor / Object	Old value	New value																			
Editor / Object	Old value	New value																					

Jetzt den JobServiceConfigurator öffnen.

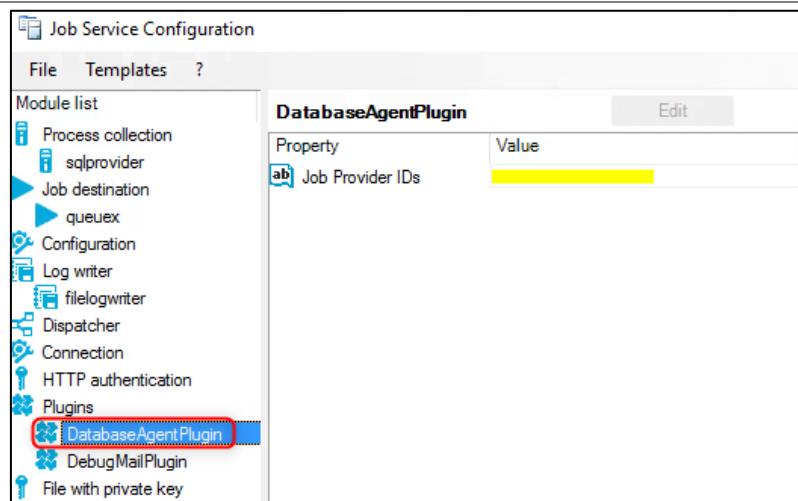


1. Ins Unterkapitel «sqlprovider» wechseln
2. Einen Connection string hinzufügen (3.)
4. Den SQL-Server und den entsprechenden SQL-Admin-User eintragen
5. Verbindung prüfen bzw. prüfen, ob die Angaben korrekt eingegeben wurden
6. Bestätigen

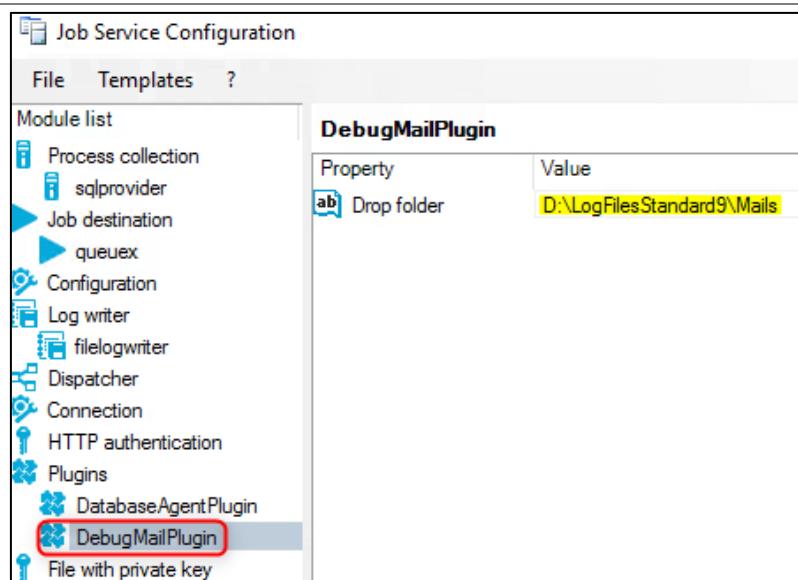


<p>Bei «Configuration» muss man noch den Port auf 1881, da bereits eine andere IAM-Installation auf dem Server über 1880 läuft.</p>	
<p>Kurz in den Explorer wechseln und folgende Ordner erstellen:</p>	
<p>Nun unter «filelogwriter» den Ordnerpfad für die Logs angeben und die maximale Parameterlänge der Logs auf 1024 erhöhen.</p>	
<p>Plugins hinzufügen.</p>	
<p>Die folgenden beiden Module nacheinander hinzufügen.</p>	

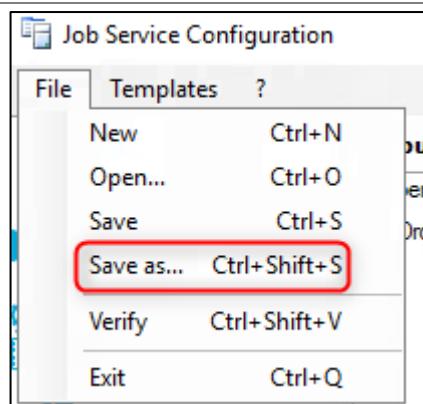
Hierbei kann der Wert leer gelassen werden, da somit der erste Job-Server verwendet wird.



Jetzt kann auch noch der Ordnerpfad des erstellten Mail-Ordners angegeben werden.



Die Konfiguration ins Installationsverzeichnis speichern.



	<p>JobService.cfg Config File (*.cfg)</p> <p>Save</p>
	<p>Services öffnen.</p> <p>Nun kann der Job-Service gestartet werden.</p>
	<p>Die JobQueueInfo öffnen und warten, bis alle Jobs durchgelaufen sind. Danach den Designer öffnen.</p>
<p>Im Designer unter «Add Job server» den eingetragenen Job-Server nach Suva-Standard anpassen.</p>	<p>CH\OIMStandard9PA (Main Database)</p> <p>Job servers: JOBSERVICE01</p> <p>Properties: Server (JOBSERVICE01), Executing server (suvanet60.ch), Parent Job server (JOBSERVICE01), Queue (JOBSERVICE01)</p>
<p>Jetzt müssen die Änderungen nur noch auf der Datenbank gespeichert werden, indem man hier noch einen «Commit to database» ausführt.</p>	<p>Designer - .SUVANET</p> <p>Commit to database</p>

<p>Je nach Änderung der Konfiguration kann es sein, dass man nach einem «Commit to database» die Datenbank kompilieren muss.</p>	

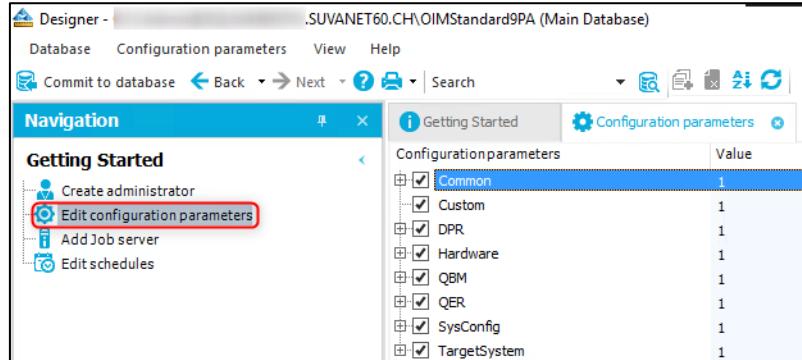
<p>Im JobServiceConfigurator im Unterkapitel «queue» die eingetragene Queue nach Suva-Standard anpassen und speichern.</p>	
<p>Nun kann der Service neugestartet werden.</p>	

Um zu überprüfen, ob der Job-Service auch tatsächlich fehlerfrei funktioniert, kann man eine Webansicht anhand der FQDN des Servers und des Ports aufrufen:

```

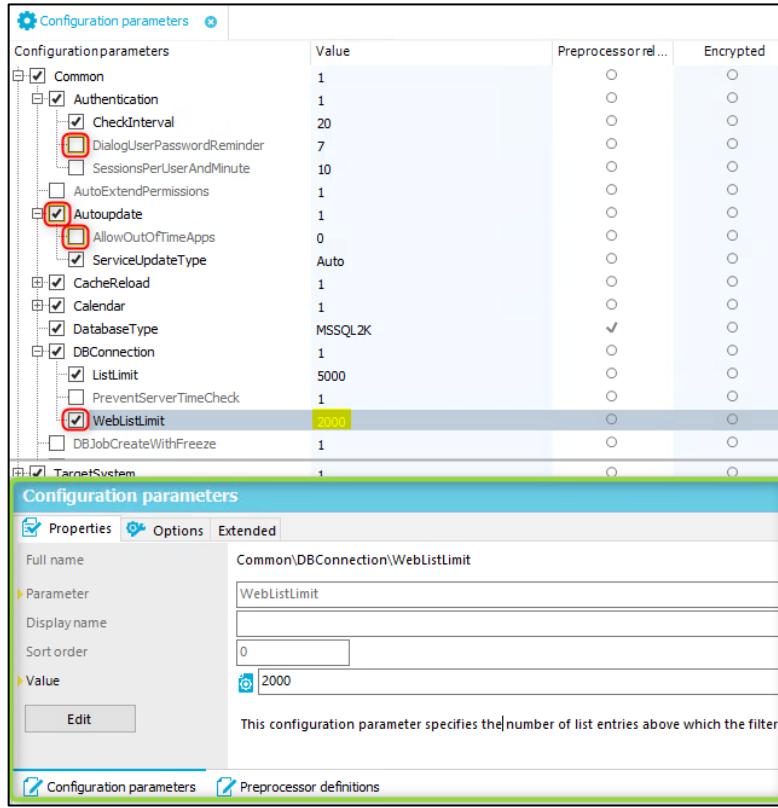
1926 2023-02-28 15:42:11 +01:00 - Info: Last process step request succeeded.
1927 2023-02-28 15:42:27 +01:00 - Info: Requesting process steps for queue "\JOBSERVICE01".
1928 2023-02-28 15:42:27 +01:00 - Info: Last process step request succeeded.
1929 2023-02-28 15:42:42 +01:00 - Info: Requesting process steps for queue "\JOBSERVICE01".
1930 2023-02-28 15:42:42 +01:00 - Info: Last process step request succeeded.
1931 2023-02-28 15:42:57 +01:00 - Info: Requesting process steps for queue "\JOBSERVICE01".
1932 2023-02-28 15:42:57 +01:00 - Info: Last process step request succeeded.
1933 2023-02-28 15:43:12 +01:00 - Info: Requesting process steps for queue "\JOBSERVICE01".
1934 2023-02-28 15:43:12 +01:00 - Info: Last process step request succeeded.
1935 2023-02-28 15:43:27 +01:00 - Info: Requesting process steps for queue "\JOBSERVICE01".
1936 2023-02-28 15:43:27 +01:00 - Info: Last process step request succeeded.
1937 2023-02-28 15:43:42 +01:00 - Info: Requesting process steps for queue "\JOBSERVICE01".
1938 2023-02-28 15:43:42 +01:00 - Info: Last process step request succeeded.
    
```

4.2 Config. Parameter konfigurieren

Schritt	Visuelle Darstellung
Im Designer können nun die Config. Parameters konfiguriert werden.	

Die rot umrandeten Config. Parameter müssen wie unten abgebildet jeweils angepasst werden. Wenn die Parameter nicht nur «de-/aktiviert werden müssen, sondern zusätzlich noch der Wert angepasst werden muss, ist dies gelb markiert.

Wie Werte von Config. Parameter angepasst werden können, ist im grün markierten Bereich ersichtlich.



<input checked="" type="checkbox"/> Journal	1		
<input checked="" type="checkbox"/> MailNotification	1		
<input type="checkbox"/> AcceptSelfSignedCert	1		
<input type="checkbox"/> AllowServerNameMismatchInCert	1		
<input checked="" type="checkbox"/> DefaultAddress	cc.iam.intern.lab60@suva.ch		
<input checked="" type="checkbox"/> DefaultCulture	en-US		
<input checked="" type="checkbox"/> DefaultFont	Times New Roman		
<input checked="" type="checkbox"/> DefaultFontSize	12		
<input checked="" type="checkbox"/> DefaultLanguage	english		
<input checked="" type="checkbox"/> DefaultSenderId	noreply@suva.ch		
<input type="checkbox"/> Encrypt	1		
<input type="checkbox"/> NotifyAboutRequestStall	1		
<input checked="" type="checkbox"/> NotifyAboutWaitingJobs	FROZEN and OVERLIMIT		
<input checked="" type="checkbox"/> Signature	1		
<input checked="" type="checkbox"/> Caption	Suva Identity und Accessmanagement		
<input checked="" type="checkbox"/> Company	Suva		
<input checked="" type="checkbox"/> Link	https:// suvanet60.ch/ITShop		
<input checked="" type="checkbox"/> LinkDisplay	IAM Portal		
<input type="checkbox"/> SignCertificateThumbprint	<Thumbprint of signing certificate>		
<input checked="" type="checkbox"/> SMTPAccount	CC.IAM.Intern.Lab60		
<input checked="" type="checkbox"/> SMTPDomain	suva.ch		
<input type="checkbox"/> SMTPPassword	<*****>		✓
<input checked="" type="checkbox"/> SMTPPort	25		
<input checked="" type="checkbox"/> SMTPRelay	localhost		
<input checked="" type="checkbox"/> MailNotification	1		
<input checked="" type="checkbox"/> ProcessState	1		
<input checked="" type="checkbox"/> Delete	1		
<input checked="" type="checkbox"/> ExportPolicy	HDB		
<input checked="" type="checkbox"/> JobHistory	ALL		
<input checked="" type="checkbox"/> Delete	1		
<input checked="" type="checkbox"/> BulkCount	200		
<input checked="" type="checkbox"/> TotalCount	10000		
<input type="checkbox"/> IsToExport	1		
<input checked="" type="checkbox"/> LifeTime	30		
<input checked="" type="checkbox"/> TrimLongParameters	10000		
<input checked="" type="checkbox"/> PackageSizeHDB	10000		
<input checked="" type="checkbox"/> ProgressView	2		
<input checked="" type="checkbox"/> Delete	1		
<input checked="" type="checkbox"/> IsToExport	1		
<input checked="" type="checkbox"/> LifeTime	30		
<input checked="" type="checkbox"/> PropertyLog	1	✓	
<input checked="" type="checkbox"/> AllDefaultPropertiesForModel	1		
<input type="checkbox"/> AutoTrackAlternatePK	1		
<input checked="" type="checkbox"/> Delete	1		
<input checked="" type="checkbox"/> IsToExport	1		
<input checked="" type="checkbox"/> LifeTime	30		
<input checked="" type="checkbox"/> ShowEffectiveAssignmentsOnly	1		
<input checked="" type="checkbox"/> DPR	1		
<input checked="" type="checkbox"/> Journal	1		
<input checked="" type="checkbox"/> StartSequence	1		
<input checked="" type="checkbox"/> UI	1		
<input checked="" type="checkbox"/> EncryptedValueHandling	ByUser		

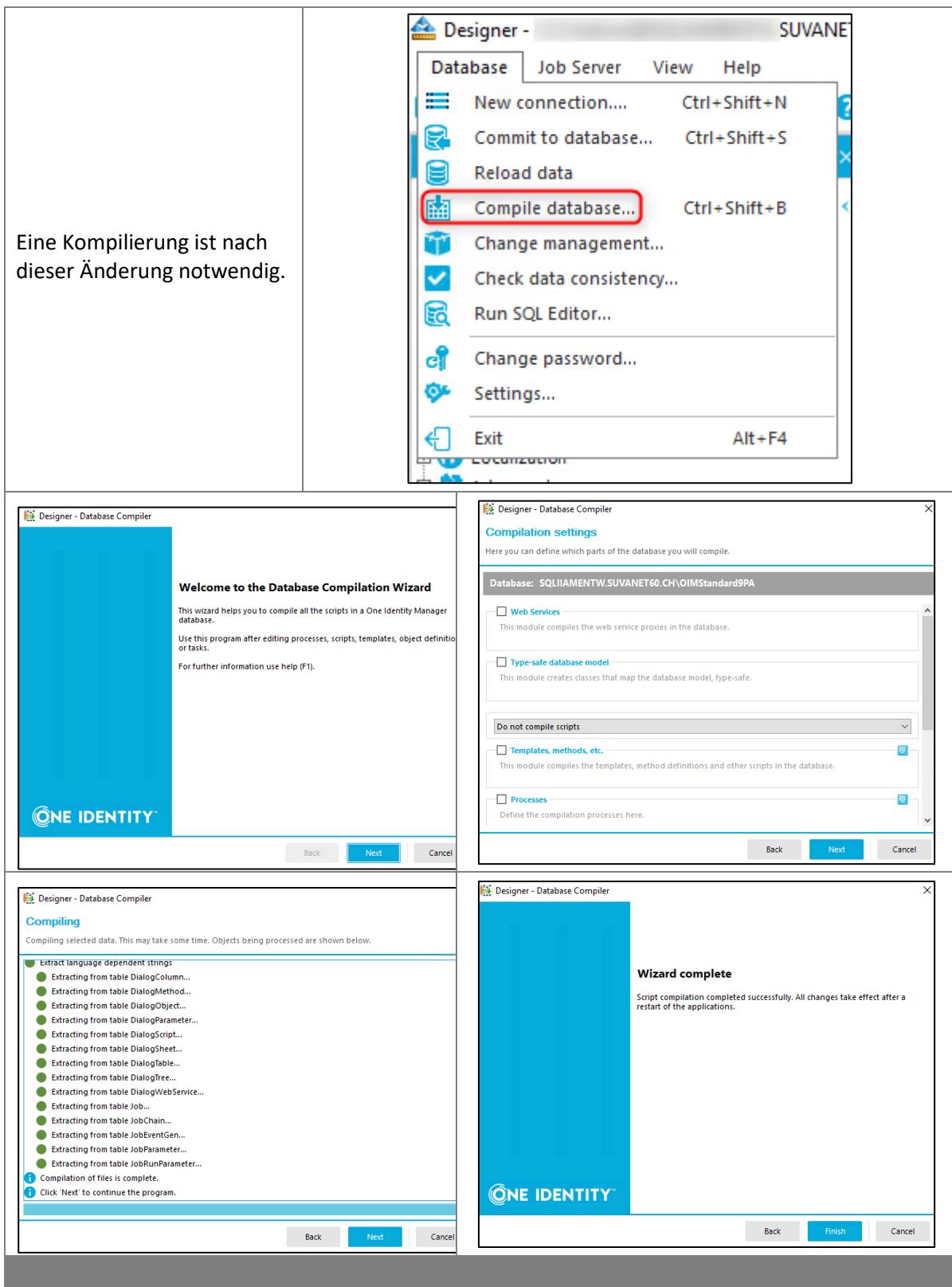
Hardware C						
<input checked="" type="checkbox"/>	QBM	1				
<input checked="" type="checkbox"/>	ApiServer	1				
<input checked="" type="checkbox"/>	AppServer	1				
<input type="checkbox"/>	DBQueue	1				
<input checked="" type="checkbox"/>	BufferTimeout	120				
<input checked="" type="checkbox"/>	ChangeLimitMax	30000				
<input checked="" type="checkbox"/>	ChangeLimitMin	3000				
<input checked="" type="checkbox"/>	CountSlotsMax	7				
<input checked="" type="checkbox"/>	DefaultRuntime	90				
<input type="checkbox"/>	GenProcIDReplaceLimit	2000				
<input checked="" type="checkbox"/>	KeepAlive	40				
<input checked="" type="checkbox"/>	DBServerAgent	1				
<input checked="" type="checkbox"/>	DBServerProperties	1				
<input checked="" type="checkbox"/>	CountCoresPerSocket	0				
<input checked="" type="checkbox"/>	CountCoresTotal	0				
<input checked="" type="checkbox"/>	CountLogicalProcessorsPerSocket	6				
<input checked="" type="checkbox"/>	CountLogicalProcessorsTotal	12				
<input checked="" type="checkbox"/>	CountSockets	2				
<input checked="" type="checkbox"/>	TimeZoneInformation	W. Europe Standard Time				
<input type="checkbox"/>	DebugMode	1				
<input type="checkbox"/>	FastUpdateDeltaOnly	CCC				
<input checked="" type="checkbox"/>	HelpLinks	1				
<input checked="" type="checkbox"/>	HtmlDevelopment	1				
<input checked="" type="checkbox"/>	ImxClient	1				
<input checked="" type="checkbox"/>	PendingChange	1				
<input checked="" type="checkbox"/>	LifeTimeError	10				
<input checked="" type="checkbox"/>	LifeTimeRunning	15				
<input checked="" type="checkbox"/>	LifeTimeSuccess	2				
QER						
<input checked="" type="checkbox"/>	Attestation	1		✓		
<input type="checkbox"/>	AERoleApproval	1		○		
<input type="checkbox"/>	AllowAllReportTypes	1		○		
<input checked="" type="checkbox"/>	ApproveNewExternalUsers	1		○		
<input checked="" type="checkbox"/>	AutoCloseInactivePerson	1		○		
<input checked="" type="checkbox"/>	AutoCreateChangeRequests	1		○		
<input checked="" type="checkbox"/>	AutoRemovalScope	1		○		
<input checked="" type="checkbox"/>	AFRoleMembership	1		○		
<input checked="" type="checkbox"/>	GroupMembership	1		○		
<input type="checkbox"/>	RemoveDelegatedRole	1		○		
<input checked="" type="checkbox"/>	RemoveDirect	1		○		
<input checked="" type="checkbox"/>	RemoveDirectRole	1		○		
<input type="checkbox"/>	RemoveDynamicRole	1		○		
<input type="checkbox"/>	RemovePrimaryRole	1		○		
<input checked="" type="checkbox"/>	RemoveRequested	1		○		
<input type="checkbox"/>	RemoveRequestedRole	1		○		
<input type="checkbox"/>	RemoveSystemRole	1		○		
<input checked="" type="checkbox"/>	LocalityInFCast	1		○		
<input checked="" type="checkbox"/>	UNSGroupInUNSGroup	1		○		
<input checked="" type="checkbox"/>	DefaultSenderAddress	compliance@suva60.ch		○		
<input type="checkbox"/>	DepartmentApproval	1		○		

<input checked="" type="checkbox"/> MailTemplateIdents	1	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> AnswerToApprover	Attestation - answer	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> RemindApproverByObject	Attestation - remind approver of all ...	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> RequestApproverByCollection	Attestation - pending attestations fo...	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> NewExternalUserFinalTimeoutInH...	24	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> NewExternalUserTimeoutInHours	4	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> OnWorkflowAssign	CONTINUE	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> OnWorkflowUpdate	CONTINUE	<input type="radio"/>	<input type="radio"/>
+ <input checked="" type="checkbox"/> OrgApproval	1	<input type="radio"/>	<input type="radio"/>
+ <input checked="" type="checkbox"/> PeerGroupAnalysis	1	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> PersonToAttestNoDecide	1	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> PrepareAttestationTimeout	48	<input type="radio"/>	<input type="radio"/>
+ <input type="checkbox"/> ProfitCenterApproval	1	<input type="radio"/>	<input type="radio"/>
+ <input checked="" type="checkbox"/> UserApproval	1	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/> UseWorkingHoursDefinition	1	<input type="radio"/>	<input type="radio"/>
+ <input checked="" type="checkbox"/> CalculateRiskIndex	1	<input checked="" type="checkbox"/>	<input type="radio"/>
+ <input checked="" type="checkbox"/> ComplianceCheck	1	<input checked="" type="checkbox"/>	<input type="radio"/>
<input type="checkbox"/> CalculateImmediately	1	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> DisableSelfExceptionGranting	1	<input type="radio"/>	<input type="radio"/>
+ <input checked="" type="checkbox"/> EmailNotification	1	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> EnableITSettingsForRule	1	<input type="radio"/>	<input type="radio"/>
+ <input checked="" type="checkbox"/> IncludeTSBPersonUsesAccount	1	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> ITShop	1	<input checked="" type="checkbox"/>	<input type="radio"/>
<input type="checkbox"/> AutoCloseInactivePerson	1	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> AutoDecision	AllStepsNoJump	<input type="radio"/>	<input type="radio"/>
+ <input checked="" type="checkbox"/> AutoPublish	1	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> ADSGroup	1	<input checked="" type="checkbox"/>	<input type="radio"/>
<input type="checkbox"/> AutoFillDisplayName	1	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> ExcludeList	[REDACTED]	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/> ChallengeRoleRemoval	1	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> DecisionOnInsert	1	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> DefaultSenderIdAddress	noreply@suva60.ch	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> Delegation	1	<input checked="" type="checkbox"/>	<input type="radio"/>
<input checked="" type="checkbox"/> Person	1	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/> AllowLoginWithSecurityIncident	1	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/> Starling	1	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> TemporaryDeactivation	1	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> UseCentralPassword	1	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> User	1	<input type="radio"/>	<input type="radio"/>
+ <input checked="" type="checkbox"/> Policy	1	<input checked="" type="checkbox"/>	<input type="radio"/>
<input checked="" type="checkbox"/> EmailNotification	1	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> DefaultSenderIdAddress	noreply@suva60.ch	<input type="radio"/>	<input type="radio"/>
+ <input checked="" type="checkbox"/> RPS	1	<input checked="" type="checkbox"/>	<input type="radio"/>
<input checked="" type="checkbox"/> DefaultReportTemplate	VI_Reportng_DefaultTemplate	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> DefaultSenderIdAddress	noreply@suva60.ch	<input type="radio"/>	<input type="radio"/>
+ <input checked="" type="checkbox"/> MailTemplateIdents	1	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> Structures	1	<input type="radio"/>	<input type="radio"/>
+ <input checked="" type="checkbox"/> WebPortal	1	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/> BaseURL	http://<server>/<App>	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> DisplayName	IAM Portal	<input type="radio"/>	<input type="radio"/>

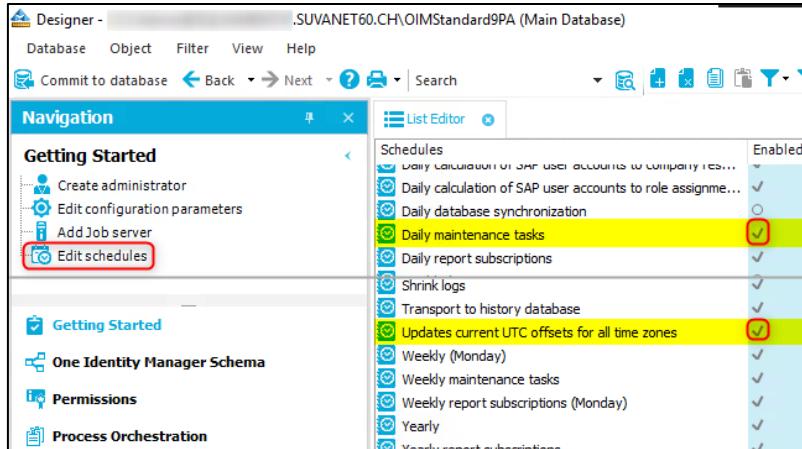
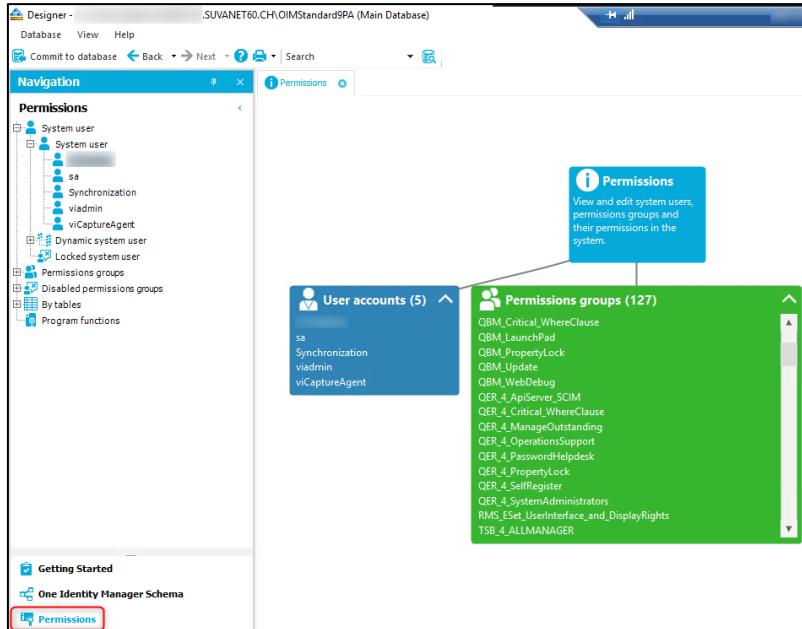
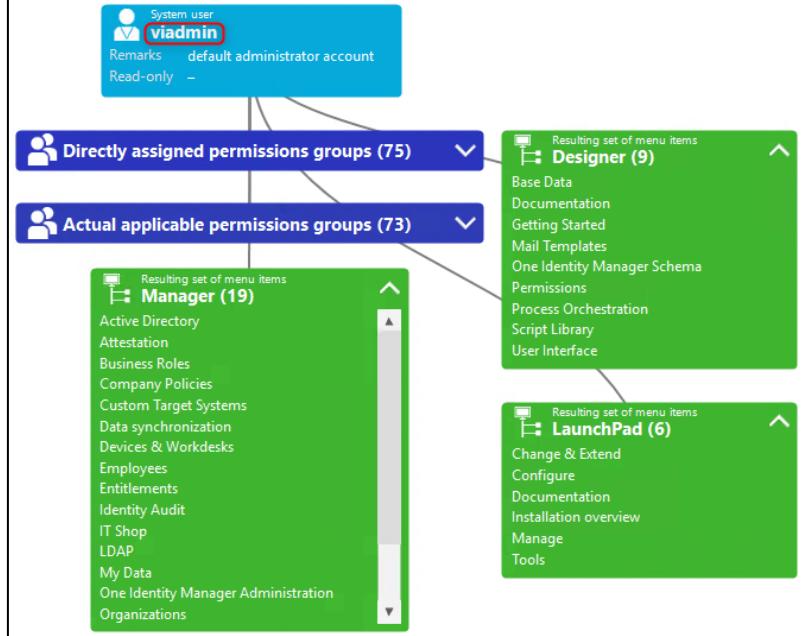
The screenshot shows four configuration windows for different target systems (TargetSystem, LDAP, SAPR3, UNS) in a software interface. Each window displays a tree view of configuration options with checkboxes. Some specific checkboxes are highlighted with red boxes:

- TargetSystem**: The 'InitialRandomPassword' checkbox under 'Accounts' is checked and highlighted.
- LDAP**: The 'InitialRandomPassword' checkbox under 'Accounts' is checked and highlighted.
- SAPR3**: The 'PersonAutoFullSync' checkbox under 'Accounts' is checked and highlighted.
- UNSA**: The 'InitialRandomPassword' checkbox under 'Accounts' is checked and highlighted. The 'SendTo' checkbox under 'Accounts' is also highlighted.

Below these windows, a message in German states that changes must still be committed to the database. To the right, a 'Designer' interface window is shown with a red box around the 'Commit to database' button. A status bar at the bottom indicates 'Save changed objects to the database.' and a table for saving changes.



4.3 Passwort-Richtlinien und Routine Tasks

Schritt	Visuelle Darstellung
Kontrollieren, ob die Schedules eingeschaltet sind.	
Im Abschnitt «Permissions» können die System-Benutzer eingesehen werden.	
Hier kann man erblicken, dass der nach dem Suva-Standard erstellte Benutzer dieselben Berechtigungen wie der Benutzer «viadmin» hat.	



Im Unterkapitel, welches rechts abgebildet ist, sind die Passwort-Richtlinien zu finden. Die Richtlinien für den Identity Manager können so gelassen werden wie sie bereits sind, da die Standardeinstellungen bereits genügend Sicherheit mit sich bringen.

The screenshot shows the SAP Designer interface for the database "SUVANET60.CH\OIMStandard9PA (Main Database)". The left navigation pane is titled "Navigation" and includes sections for "Base Data", "Security settings", "Database server permissions", and "Password policies". The "Password policies" section is highlighted with a red box. The main content area displays a table titled "Password policies" with the following data:

	Description
Active Directory password policy	Predefined password policy for Active Directory user passwords.
LDAP password policy	Predefined password policy for LDAP user passwords.
One Identity Manager password policy	Predefined password policy for system user passwords to authenticate on %Global.QIM_ProductNameShort%.
Password policy for central password of employees	Predefined password policy for the central password of employees.
SAP R/3 password policy	Predefined password policy for SAP R/3 user passwords.

The "One Identity Manager password policy" row is selected and shown in detail in the bottom half of the screen. The "Getting Started" section of the navigation bar is also highlighted with a red box.

Für die Richtlinien im LDAP werden folgende Anpassungen nach Suva-Standard vorgenommen.

The screenshot shows the OIM Designer application with the following details:

- Navigation Bar:** Database, Object, Filter, View, Help, Commit to database, Back, Next, Search.
- Left Sidebar:** Base Data (General, Security settings, Authentication modules, Database server permissions), OAuth 2.0/OpenID Connect configuration, Password policies, Restricted passwords.
- Central Area:**
 - Base Data - Password policies:** A list of policies including Active Directory password policy, LDAP password policy (selected and highlighted with a red box), One Identity Manager password policy, Password policy for central password of employees, and SAP R/3 naesword policy.
 - LDAP password policy Configuration:** A detailed configuration panel with tabs for Password, Character classes, Scripts, Test, and Assignments.
 - Initial password:** Two masked input fields.
 - Confirmation:** Two masked input fields.
 - Min. length:** Set to 0.
 - Max. length:** Set to 0.
 - Max. failed logins:** Set to 180.
 - Max. days valid:** Set to 90.
 - Password history:** Set to 0.
 - Min. password strength:** Set to 0.
 - Prohibited name properties:** An unchecked checkbox.

5 Implementation

Schritt	Visuelle Darstellung
Im Manager unter «LDAP» eine Account Definition erstellen.	<p>The screenshot shows the LDAP Manager interface. On the left, there's a tree view with 'Info system', 'Hierarchical view', 'Domains' (selected), 'Container', and 'User accounts'. Below the tree are sections for 'Employees', 'Organizations', 'Business Roles', and 'Custom Target Systems'. At the bottom are navigation icons: HDS, LDRP (highlighted in yellow), SHP, and others. On the right, a 'Tasks' panel lists 'Tasks' (checked) and 'Create account definition...'. The 'Create account definition...' item is highlighted with a red box.</p>
Die Account Definition sollte dann etwa wie folgt aussehen:	<p>The screenshot shows the 'Create account definition...' dialog. It has several fields: 'Account definition' set to 'LDAP_CreateAccount', 'User account table' set to 'LDAPAccount', 'Required account definition' (empty), and 'Manage level (initial)' set to 'Full managed'. Under 'Advanced settings', three checkboxes are checked and highlighted with red boxes: 'Retain account definition if temporarily disabled', 'Retain account definition on deferred deletion', and 'Retain account definition on security risk'. At the bottom, there's a section about inheritance: 'Groups can be inherited' with radio buttons for 'Yes' (selected), 'No', and 'Not specified'. The 'Yes' button is also highlighted with a red box. At the very bottom are 'Ok' and 'Cancel' buttons.</p>
Unter «Entitlements» eine Mapping Rule auf der Account Definition erstellen.	<p>The screenshot shows the Entitlements Manager interface. On the left, there's a tree view with 'Info system', 'Active Directory groups', 'Assignment resources for IT Shop' (selected), 'Account definitions', 'Report subscriptions', and 'Basic configuration data'. Below the tree are sections for 'Employees', 'Organizations', 'Business Roles', and 'Entitlements' (highlighted in yellow). At the bottom are navigation icons: HDS, LDRP, SHP, and others. On the right, a 'Tasks' panel lists various tasks. The 'Edit IT operating data mapping rule' item is highlighted with a red box.</p>

<p>Hier ein neues Mapping hinzufügen.</p>	<div style="border: 1px solid #ccc; padding: 5px;"> <p>General</p> <p>Mappings Add <input type="button" value="Add"/> Remove</p> <p>Column <input type="text" value="LDAPAccount.IsGroupAccount"/></p> <p>Column <input type="text" value="LDAPAccount - UID_LDAPContainer"/> ▼</p> <p>Source <input type="text" value="Primary department"/> ▼</p> <p>Default value <input type="text" value="Import (suvanet60.ch/ldap10/Test/Users/Import)"/> ▼</p> <p><input type="checkbox"/> Always use default value</p> <p><input type="checkbox"/> Notify when applying the default</p> </div>
---	--

Als Nächstes unter «Business Roles» eine neue Role Class erstellen.

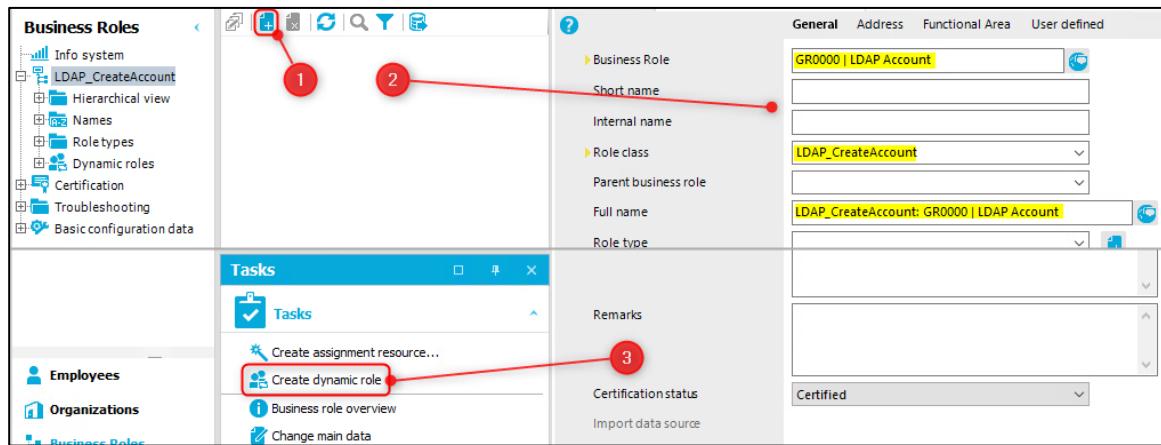
	<div style="border: 1px solid #ccc; padding: 5px;"> <p>General</p> <p>Role class <input type="text" value="LDAP_CreateAccount"/> Edit <input type="button" value="Edit"/></p> <p>Role type <input type="text"/> Edit <input type="button" value="Edit"/></p> <p>Attestor <input type="text"/> Edit <input type="button" value="Edit"/></p> <p>Description <input type="text"/></p> <p><input checked="" type="radio"/> Inherited top down <input type="radio"/> Inherited bottom up</p> <p><input type="checkbox"/> Delegable</p> <p><input type="checkbox"/> No multiple assignment of employees</p> </div>
--	---

<p>Nach einem Refresh (F5) sollte die Role Class ersichtlich sein. Auf dieser werden nun die Role Assignments konfiguriert</p>	
--	--

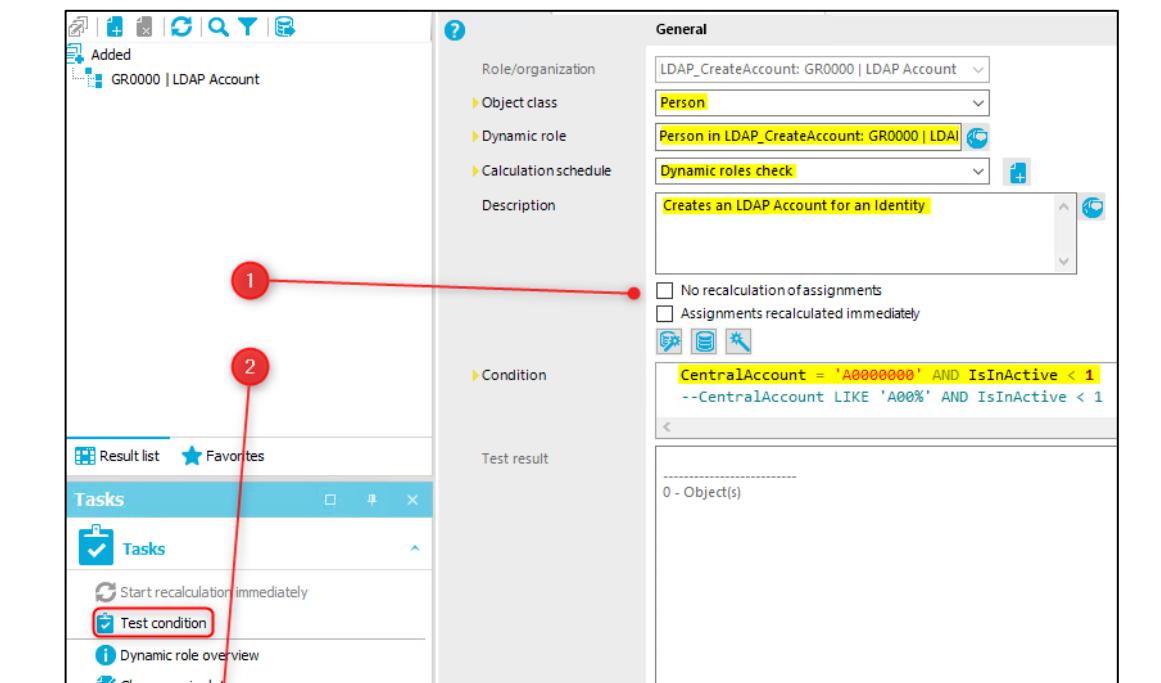
<div style="border: 1px solid #ccc; padding: 5px;"> <p>Tasks</p> <p><input checked="" type="checkbox"/> Tasks Edit <input type="button" value="Edit"/></p> <p><input type="checkbox"/> Role class overview</p> <p><input type="checkbox"/> Change main data Edit <input type="button" value="Edit"/></p> <p><input type="checkbox"/> Configure role assignments Edit <input type="button" value="Edit"/></p> <p><input type="checkbox"/> Assign role types</p> </div>

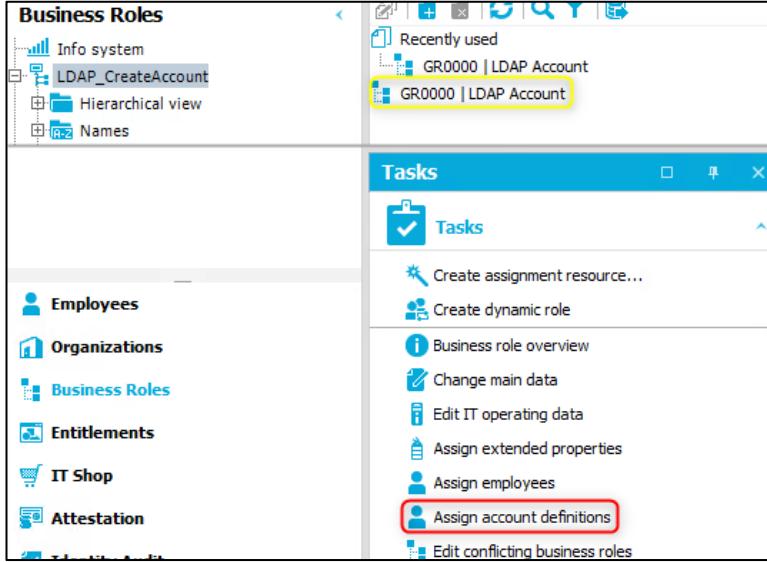
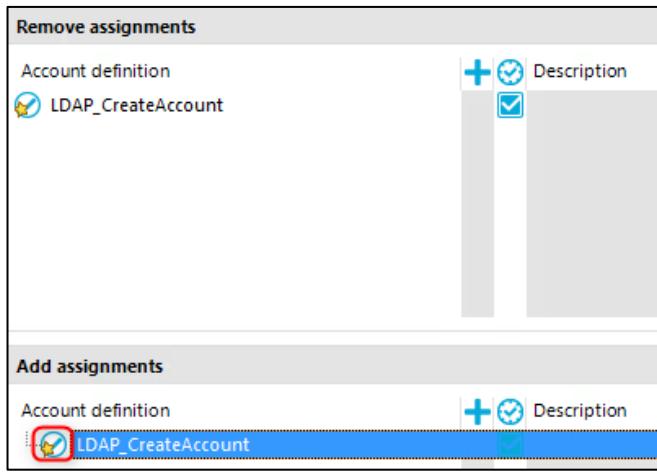
<p>Hierbei «Account Definitions» und «Employees» auswählen.</p>	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">Roleassignments</th> <th style="width: 10%; text-align: center;">Assignments ...</th> <th style="width: 10%; text-align: center;">Direct assig...</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> Account definitions</td> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td><input type="checkbox"/> Active Directory groups</td> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td><input type="checkbox"/> Assignment resources</td> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td><input type="checkbox"/> Devices</td> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td><input type="checkbox"/> Employees</td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td><input type="checkbox"/> Groups</td> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td><input type="checkbox"/> LDAP groups</td> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td><input type="checkbox"/> Multi requestable/unsubscribable resources</td> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td><input type="checkbox"/> Multi-request resources</td> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td><input type="checkbox"/> Resources</td> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> </tbody> </table>	Roleassignments	Assignments ...	Direct assig...	<input type="checkbox"/> Account definitions	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/> Active Directory groups	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Assignment resources	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Devices	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Employees	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/> Groups	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> LDAP groups	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Multi requestable/unsubscribable resources	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Multi-request resources	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Resources	<input type="checkbox"/>	<input type="checkbox"/>
Roleassignments	Assignments ...	Direct assig...																																
<input type="checkbox"/> Account definitions	<input type="checkbox"/>	<input checked="" type="checkbox"/>																																
<input type="checkbox"/> Active Directory groups	<input type="checkbox"/>	<input type="checkbox"/>																																
<input type="checkbox"/> Assignment resources	<input type="checkbox"/>	<input type="checkbox"/>																																
<input type="checkbox"/> Devices	<input type="checkbox"/>	<input type="checkbox"/>																																
<input type="checkbox"/> Employees	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>																																
<input type="checkbox"/> Groups	<input type="checkbox"/>	<input type="checkbox"/>																																
<input type="checkbox"/> LDAP groups	<input type="checkbox"/>	<input type="checkbox"/>																																
<input type="checkbox"/> Multi requestable/unsubscribable resources	<input type="checkbox"/>	<input type="checkbox"/>																																
<input type="checkbox"/> Multi-request resources	<input type="checkbox"/>	<input type="checkbox"/>																																
<input type="checkbox"/> Resources	<input type="checkbox"/>	<input type="checkbox"/>																																

Als Nächstes eine Geschäftsrolle auf der erstellten Role Class hinzufügen. Diese hat die Namenskonvention «GRXXXX | YZ» nach Suva-Standard. Danach aus dieser GR eine dynamische Rolle erstellen.



Hier kann gefiltert werden, welche Identitäten die Geschäftsrolle automatisch erhalten sollen und somit für welche Identitäten ein LDAP Account erstellt werden muss. Die Filterung kann dann gleich getestet werden.



<p>Zum Schluss muss die erstellte Account Definition noch der GR zugewiesen werden.</p>	 <p>The screenshot shows the 'Business Roles' interface. On the left, there's a navigation tree with 'Info system', 'LDAP_CreateAccount' (selected), 'Hierarchical view', and 'Names'. Below the tree are links for 'Employees', 'Organizations', 'Business Roles' (selected), 'Entitlements', 'IT Shop', and 'Attestation'. On the right, there's a 'Recently used' list with 'GR0000 LDAP Account' (selected) and 'GR0000 LDAP Account'. A 'Tasks' panel is open, listing various options: 'Tasks' (selected), 'Create assignment resource...', 'Create dynamic role', 'Business role overview', 'Change main data', 'Edit IT operating data', 'Assign extended properties', 'Assign employees', 'Assign account definitions' (highlighted with a red box), and 'Edit conflicting business roles'.</p>
<p>Mit einem Doppelklick kann hier die Account Definition ausgewählt werden.</p>	 <p>The screenshot shows two panels: 'Remove assignments' and 'Add assignments'. In the 'Remove assignments' panel, there's a table with one row for 'LDAP_CreateAccount'. In the 'Add assignments' panel, there's a table with one row for 'LDAP_CreateAccount', which is highlighted with a blue selection bar.</p>

Besprechungsprotokoll: Expertenbesuch

Thema der Besprechung:

Erstbesuch des Hauptexperten Florian Reck

Datum / Uhrzeit:

27.02.2023 16:00

Ort / Raum:

MS Teams (virtuell)

Teilnehmende:

Dätwyler, Mike

Stadelmann, Andreas

Reck, Florian

Besprechungspunkte

Formalitäten

- Vorstellung
- Anredeform → per du
- Bei Notfall beim Hauptexperten, dann beim Zweitexperten und dann Sekretariat melden

Dokumentation

- Inhaltsverzeichnis zeigen
- Arbeitsjournal zeigen
- Projektplanung zeigen

Präsentation

- Sprache der Präsentation → Mundart
- Präsentationstermin → 21.03.2023 08:30
 - vorgängige Parkplatz-Reservation
- Dauer der Präsentation = 15-20 Minuten
- Dauer der Demo = 10 Minuten
- Dauer des Fachgesprächs = max. 30 Minuten

Abgabe

- bis 18:00 muss abgegeben sein
- lieber früher abgeben → hoher Traffic

Hinweise

- besondere Acht beim Testkonzept
- Lifecycle von One Identity ansehen → Support-Dauer für Identity Manager Version