|  |
| --- |
| identity management active directory |
| Technische Dokumentation  <Webbasiertes Reporting von Userberechtigungen für Windows Active Directory - WRAD>  **Projektteam 2/3**  Dario Furigo  Philipp Köfer  Nicola Michaelis  Beat Schärz  **V0.2**  16.01.2019 |
| **Berner Fachhochschule**  Departement für Technik und Informatik |

Inhaltsverzeichnis

[1 Versionskontrolle 2](#_Toc533328946)

[2 Referenzierte Dokumente 2](#_Toc533328947)

[3 Zweck des Dokuments 2](#_Toc533328948)

[4 Applikationsfunktion 3](#_Toc533328949)

[4.1 Einschränkungen / Entscheidungen 3](#_Toc533328950)

[5 Architektur 3](#_Toc533328951)

[6 Module 5](#_Toc533328952)

[6.1 Modulname: Datencontainer 5](#_Toc533328953)

[6.2 Modulname: IST-SOLL Vergleich 5](#_Toc533328954)

[6.3 Modulname: Reporting 5](#_Toc533328955)

[6.4 Modulname: Auditing 5](#_Toc533328956)

[6.5 Modulname: History 5](#_Toc533328957)

[6.6 Modulname: Auslesen der Daten (Rohdaten) 5](#_Toc533328958)

[6.7 Modulname: Testdaten (Testsystem) 5](#_Toc533328959)

[6.8 Modulname: Daten SOLL 6](#_Toc533328960)

[6.9 Modulname: Einlesen Daten SOLL 6](#_Toc533328961)

[6.10 Modulname: (OPTION) Exportieren Daten SOLL 6](#_Toc533328962)

[6.11 Modulname: (OPTION) Alarmierung 6](#_Toc533328963)

[6.12 Modulname: (OPTION) Remediation 6](#_Toc533328964)

[6.13 Modulname: (OPTION) Fileshares (Permissions) 6](#_Toc533328965)

[7 Installationsanleitung 7](#_Toc533328966)

[8 Testdokumentation 9](#_Toc533328967)

[8.1 Testfälle 9](#_Toc533328968)

[8.2 Testergebnisse 9](#_Toc533328969)

[9 Projekt Review 10](#_Toc533328970)

[10 Glossar 11](#_Toc533328971)

[11 Abbildungsverzeichnis 11](#_Toc533328972)

# Versionskontrolle

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Datum | Beschreibung | Autor |
| 0.1 | 30.11.2018 | Dokument erstellt | P.K. |
| 0.2 | 17.12.2018 | Dokument erweitert (Kapitel 3,5,6) | P.K. |
| 0.3 | 21.12.2018 | Dokument erweitert (div. Kapitel) | P.K. |
| 1.0 | 23.12.2018 | Dokument angepasst und erste Version erstellt | D.F. |

# Referenzierte Dokumente

|  |  |  |
| --- | --- | --- |
| Dokumenten Name | Zweck | Pfad |
| Anforderungsspezifikation.docx | Requirements Spezifikation | .\ ProjektMgmt\ |
| Diary.md | Protokoll Projekt-Team-Meetings | .\ |
| ImportTemplateGroup.csv | CSV Vorlage für Import Gruppen | .\ |
| ImportTemplateUser.csv | CSV Vorlage für Import User | .\ |
| Zeitplan.xlsx | Projekt Zeitplan | .\ |
| testdata.sql | Testdaten für SOLL/IST Vergleich | .\ |

# Zweck des Dokuments

In diesem Dokument wird die Technische Umsetzung und die verwendeten Technologien für das WRAD Projekt beschrieben.

Das Reportingtool ist eine webbasierte Lösung, welches Audits über ein Active Directory vereinfacht. Die Lösung ist sowohl für Systemadministratoren als auch für Manager und Auditoren nützlich. Mit den Reports werden einerseits klassische Probleme wie z.B. verwaiste Accounts ersichtlich, andererseits ist aber auch ein IST/SOLL Vergleich der Berechtigungen möglich. Weiter kann dem Tool auch eine „History“ eines Users entnommen werden, welche aufzeigt wie sich dieser User über die Zeit entwickelt hat.

# Applikationsfunktion

## Einschränkungen / Entscheidungen

### PS Universal Dashboard

Das PowerShell Framework stellte uns vor viele kleinere und grössere Probleme, da das Produkt noch in Weiterentwicklung steht, sind noch viele Bugs und nicht ausgereifte Teile vorhanden.

Zum Beispiel werden Variabeln zwischen den Seiten nicht sauber übergeben und es gibt keine einfache Möglichkeit gewisse Elemente wie Buttons darzustellen.

### Lizenz

Diverse Module, die wir verwenden wollten unterlagen Lizenzrestriktionen und waren für uns somit nicht brauchbar. Den einzigen Kompromiss gingen wir bei Universal Dashboard ein, welches kostet und nur in einer sehr eingeschränkten kostenfrei verfügbar ist.

### Import Funktion

Zum Importieren von SOLL-Daten muss .csv-File in einem spezifischen Format genutzt werden. Dazu werden das File ImportTemplateGroup.csv für den SOLL-Import von Gruppen und das File ImportTemplateUser.csv für den SOLL-Import von Usern genutzt. Durch logische Einschränkungen müssen zuerst die Gruppen und dann die User importiert werden, um die Gruppen-Mitgliedschaften sauber abbilden zu können.

# Architektur

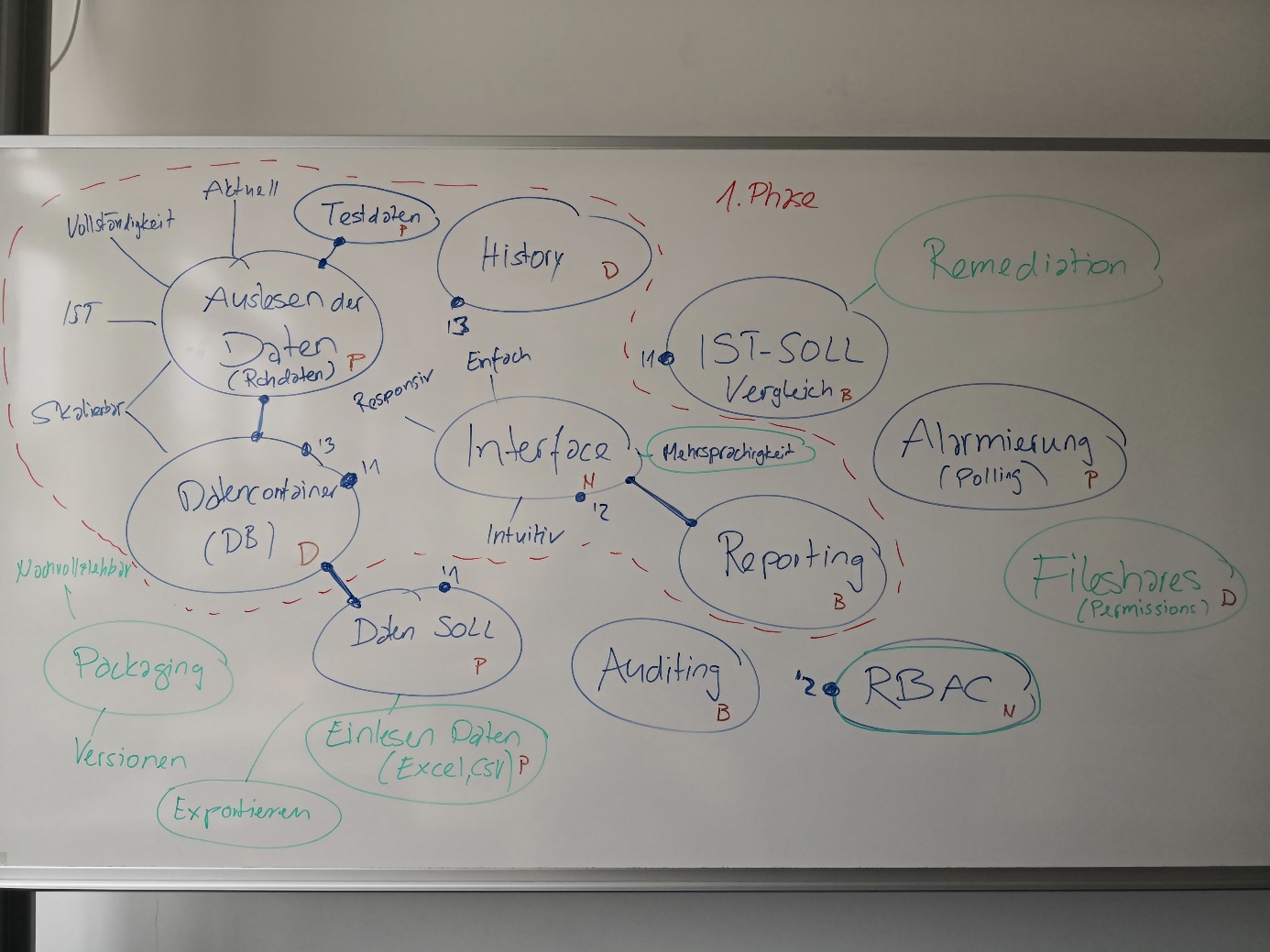


Abbildung 1: Architektur und geplante Aufteilung in Module

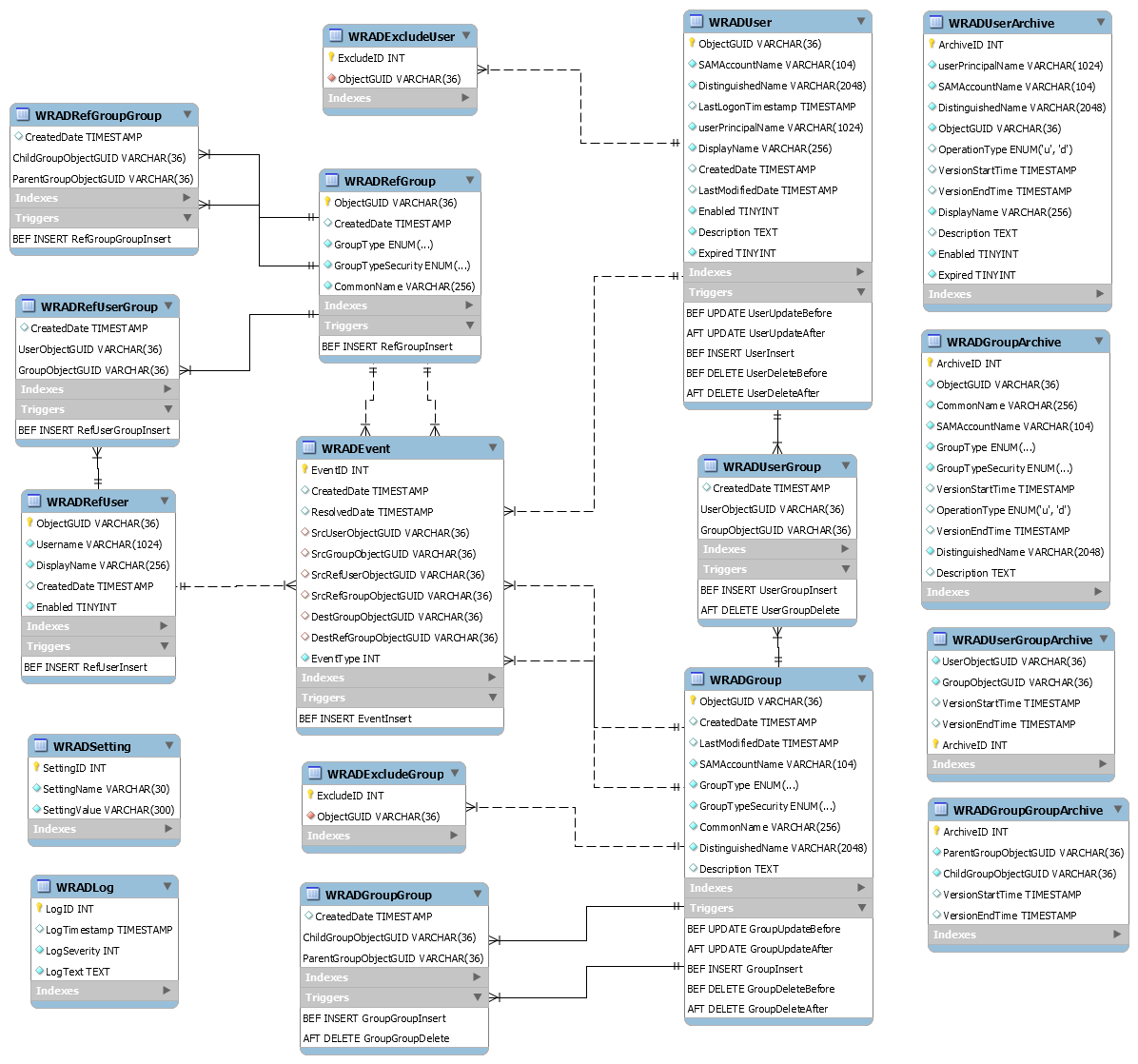


Abbildung 2: Schema der genutzten Datenbank auf dem MariaDB Server

# Module

## Modulname: Datencontainer

Kurzbeschrieb: Der Datencontainer dient dazu, die vom AD ausgelesenen IST-Daten oder vom User erfassten SOLL-Daten abzuspeichern. Diese Daten können in eine Datenbank oder als Files abgelegt werden. Dieser Datencontainer sollte skalierbar und erweiterbar sein.

Wichtige Funktionen: Speichern von Daten, Auslesen von Daten, Organisieren von Daten (Index)

Abhängigkeiten: SOLL-Daten, IST-Daten, History

## Modulname: IST-SOLL Vergleich

Kurzbeschrieb: Eine zentrale Funktion des Programms. Hier soll der gewünschte Berechtigungs-Zustand (SOLL) eingelesen und mit dem momentanen Zustand (IST) verglichen werden können. Daraus sollen dann Abweichungen der beiden Zustände ersichtlich werden.

Wichtige Funktionen: Delta der beiden Zustände eruieren.

Abhängigkeiten: Der IST-SOLL Vergleich ist primär vom Datencontainer abhängig. Dort sind sowohl IST als auch SOLL Zustand gespeichert, weswegen der Vergleich nur funktioniert, wenn diese Daten vom Datencontainer geholt werden können.

## Modulname: Reporting

Kurzbeschrieb: Reports anhand von gewünschten Einstellungen durchführen und diese in ein gewünschtes Format bringen. (Beispiel PDF). Reports sollen von Hand (per UI) oder als regelmässiger Job ausgeführt werden können.

Wichtige Funktionen: Reports generieren und verschicken.

Abhängigkeiten: Das Reporting ist teils vom UI abhängig, da darüber die Einstellungen für die Reports gemacht werden.

## Modulname: Auditing

Kurzbeschrieb: Alle Aktionen, welche im User Interface oder durch das Reporting ausgeführt werden, sollen in ein remote Log geschrieben werden. (Beispiel remote syslog Server)

Wichtige Funktionen: Logging von Reporting und User Aktionen.

Abhängigkeiten: Damit das Logging funktioniert, müssen vom Interface und vom Reporting Logs gesendet werden. Ausserdem ist ein syslog Server (oder ähnliches) benötigt.

## Modulname: History

Kurzbeschrieb: Die History stellt im Datencontainer fest, dass alle Änderungen der IST-Daten historisch nachvollziehbar sind.

Wichtige Funktionen: Auslesen der historischen Zustände und Speichern des Deltas der IST-Daten.

Abhängigkeiten: Datencontainer, IST-Daten

## Modulname: Auslesen der Daten (Rohdaten)

Kurzbeschrieb: Dieses Modul dient zum Auslesen der Rohdaten aus dem AD und anschliessendes abspeichern im Datencontainer. Diese Funktion sollte skalierbar, aktuell und vollständig sein.

Wichtige Funktionen: Auslesen von Daten, Speichern von Daten

Abhängigkeiten: Datencontainer, Rohdaten (Testdaten)

## Modulname: Testdaten (Testsystem)

Kurzbeschrieb: Eine Umgebung mit realitätsnahen Testdaten welche wir zum Entwickeln und Testen nutzen können.

Wichtige Funktionen: Testing, Entwickeln

Abhängigkeiten: keine

## Modulname: Daten SOLL

Kurzbeschrieb: Der aktuell gewünschte Berechtigungs-Zustand (SOLL) wird im Datencontainer abgespeichert.

Wichtige Funktionen: Bereitstellen des Soll-Zustandes

Abhängigkeiten: Datencontainer

## Modulname: Einlesen Daten SOLL

Kurzbeschrieb: Die Daten des gewünschten Berechtigungs-Zustands (SOLL) können von den Anwendern importiert/aktualisiert werden. Diese Daten sind in Form eines .CSV-Files vorhanden.

Wichtige Funktionen: Einlesen von .CSV-Files in den Daten SOLL

Abhängigkeiten: Datencontainer, Daten SOLL

## Modulname: (OPTION) Exportieren Daten SOLL

Kurzbeschrieb: Der aktuell in der Applikation hinterlegte Berechtigungs-Zustand (SOLL) kann in ein .CSV-File exportieren werden. Dient zum Anpassen und erneuten importieren des Berechtigungs-Zustands (SOLL).

Wichtige Funktionen: Exportieren des Daten SOLL in ein .CSV-File

Abhängigkeiten: Datencontainer, Daten SOLL

## Modulname: (OPTION) Alarmierung

Kurzbeschrieb: Ein Modul zur aktiven Alarmierung von bestimmten Administratoren bei Veränderung von Berechtigungen im AD.

Wichtige Funktionen: Alarmierung von Administratoren

Abhängigkeiten: keine

## Modulname: (OPTION) Remediation

Kurzbeschrieb: Dies ist eine Option welche in einer späteren Phase des Projekts (falls genügend Zeit vorhanden ist) eingebaut werden kann. Damit soll es möglich sein beim IST-SOLL Vergleich gewisse Deltas direkt im AD angleichen zu können.

Wichtige Funktionen: Angleichung von Differenzen der Zustände direkt im AD.

Abhängigkeiten: IST-SOLL Vergleich

## Modulname: (OPTION) Fileshares (Permissions)

Kurzbeschrieb: Dieses Modul ist optional und ermöglich das Sammeln der Berechtigungen auf definierten Files Shares. Es ermöglicht das Auditieren der Berechtigungen.

Wichtige Funktionen: Auslesen von Berechtigungen auf Fileshares

Abhängigkeiten: keine

# Installationsanleitung

Prerequisits

- .NET 4.7.2 oder höher

-- https://dotnet.microsoft.com/download/dotnet-framework-runtime

- Posh-SYSLOG 3.3

-- Powershell als Administrator:

-- Install-Module -Name Posh-SYSLOG -RequiredVersion 3.3

- Installation UniversalDashboard

-- Update von Powershellget

--- Install-Module powershellget -force

-- Installation von UniversalDashboard

--- Install-Module UniversalDashboard

- MariaDB 10.3

-- downloads.mariadb.org -> Nach passendem MSI suchen

-- Bei der Installation gewünschtes root PW setzen ansonsten Standard Werte

- MySQL Connector

-- https://dev.mysql.com/downloads/connector/net/

-- Download mysql-installer-web-community-X.X.X.X.msi

-- Custom wählen -> MYSQL Connectors -> Connector/NET -> Connector/NET X.X -> Connector/NET X.X.X - X86

-- Ansonsten Standard beibehalten

DB Schema

- Download DB Schema: https://github.com/VirtSyntaxError/BTI7301-2018-WRAD/blob/master/doc/dbschema.sql

- Import DB Schema

-- Utility HeidiSQL öffnen & Login mit vorhin gewähltem root-PW

-- Query SELECT PASSWORD('<yourPW>'); ausführen und Ergebnis kopieren

-- File -> Load SQL File -> File auswählen

-- Zeile "CREATE USER[...]": Sterne (\*\*\*) durch kopierten PW-hash ersetzen.

-- ZEILE "INSERT INTO Settings[...]" gewünschte Settingvalues setzen

-- Run Statement

-- Nun sollte eine wrad DB existieren

Installation WRAD

- Git Repo an gewünschten Ort klonen: https://github.com/VirtSyntaxError/BTI7301-2018-WRAD/tree/master/src

- Von Hand File "db\_pw.ini" im Ordner src/modules erstellen und dort das vorher gewählte <yourPW> eintragen.

Installation Tasks

- Bei jedem XML-Tasks im Ordner src/tasks die Variable %PATH% mit dem Installationspfad anpassen

- Den Task Scheduler öffnen und die 4 Tasks mit den Defaultwerten importieren

Import der bestehenden SOLL Daten

- Die Templates doc/ImportTemplateGroup.csv und doc/ImportTemplateUser.csv anpassen und die bestehenden SOLL Accounts erfassen

- Powershell öffnen und das Modul src/modules/WRADcsvSOLL.psd1 importieren

- Es müssen zuerst die Gruppen, dann die User importieren werden (logische Einschränkung durch Gruppen-Mitgliedschaften)

- Die Gruppen wie folgt importieren:

-- Import-WRADcsv -ImportAs Groups -csvPath doc/ImportTemplateGroup.csv

- Die User wie folgt importieren:

-- Import-WRADcsv -ImportAs Users -csvPath doc/ImportTemplateUser.csv

Start WRAD

- Mit Powershell src/GUI/UDGUI.ps1 ausführen

- Beim ersten Mal muss diese zwei Mal ausgeführt werden.

- Der Port auf welchem das GUI verfügbar ist wird ausgegeben

- Per Firefox auf localhost:<PORT>/login zugreifen und einloggen mit Admin:admin

# Testdokumentation

## Testfälle

Die Testfälle wurden aus den entsprechenden Funktionalen Anforderungen der Anforderungsspezifikation abgeleitet.

|  |  |
| --- | --- |
| **ID** | **Beschreibung** |
| **F2** | Auditor |
| **F2.1** | Als Auditor will ich fertige Reports zur Verfügung haben, welche ich nur noch ausführen muss, sodass ich nicht nach den Informationen suchen muss. |
| **F2.2** | Als Auditor will ich in einem Report ein Vergleich des SOLL- und IST-Zustands machen können, sodass ich falsche Berechtigungen erkenne. |
| **F2.3** | Als Auditor will ich in einem Report eine Liste von deaktivierten Usern sehen können. |
| **F2.4** | Als Auditor will ich, dass in einem Report eine Liste von inaktiven Usern ersichtlich ist. Somit sehe ich welche Benutzer sich lange nicht mehr eingeloggt haben. |
| **F2.5** | Als Auditor will ich einen Report im PDF-Format erstellen können. |
| **F3** | Systemadministrator |
| **F3.1** | Als Systemadministrator will ich auf dem Dashboard schnell für mich relevante Informationen wie die Zeit der letzten Statusabfrage sehen, sodass ich nicht danach suchen muss. |
| **F3.2** | Als Systemadministrator will ich dieselben Möglichkeiten haben wie ein Auditor. |
| **F4** | Application Owner |
| **F4.1** | Als Application Owner will ich vollen Zugriff auf alle Funktionen des Systems, sodass ich die Applikation pflegen kann. |
| **F4.2** | Als Application Owner will ich Zugriff auf ein Log, welches alle Aktionen der Anwender der Applikation loggt, so dass ich diese nachvollziehen kann. |
| **F4.3** | Als Application Owner will ich nach der Installation der Applikation einen SOLL-Zustand in einem CSV importieren können. |
| **F4.5** | Als Application Owner will ich einen SOLL-Zustand in ein CSV exportieren können. |

## Testergebnisse

|  |  |
| --- | --- |
| **ID** | **Testergebniss** |
| **F2** | Auditor |
| **F2.1** | Erfolgreich |
| **F2.2** | Erfolgreich |
| **F2.3** | Erfolgreich |
| **F2.4** | Erfolgreich |
| **F2.5** | Erfolgreich |
| **F3** | Systemadministrator |
| **F3.1** | Teilweise erfolgreich (Statusabfrage ist manuell) |
| **F3.2** | Erfolgreich |
| **F4** | Application Owner |
| **F4.1** | Erfolgreich |
| **F4.2** | Erfolgreich |
| **F4.3** | Erfolgreich |
| **F4.5** | Erfolgreich |

Zudem wurde für den SOLL/IST Vergleich das referenzierte SQL-Skript testdata.sql benutzt.

# Projekt Review

Das Auswählen des richtigen Frameworks hat uns vor eine gross Challenge gestellt. Wir waren uns alle einig, dass wir eine Systemnahe Programmier- oder Skriptsprache auswählen müssen. Dies war jedoch nicht einfach, da die Web-Frameworks für PowerShell nur sehr eingeschränkt verfügbar sind. Wir sind bei der Recherche auf UniversalDashboard gestossen, welches noch in einer aktiven Weiterentwicklung steht und viele Bugs aufweist. Diese Probleme führten auch zum Verzug diverser Meilensteine.

Wir sind der Meinung, dass das Backend zukunftsgerichtet ist, jedoch müsste man sich überlegen das Frontend mit einem anderen Framework zu realisieren.

# Glossar

|  |  |
| --- | --- |
| Begriff | Beschreibung |
| AD | Active Directory |
| CSV | Das Dateiformat CSV steht für Comma-Separated Values und beschreibt den Aufbau einer Textdatei zur Speicherung von Daten. |
| HR | Human Resources |
| MariaDB | MariaDB ist eine relationale Datenbank. |
| Verwaiste Accounts | Accounts gelten als verwaist, wenn diese über einen Zeitraum nicht mehr gebraucht werden. |
| WRAD | Webbasiertes Reporting für Windows Active Directory |

# Abbildungsverzeichnis

[Abbildung 1: Architektur und geplante Aufteilung in Module](#_Toc533164465)

[Abbildung 2: Schema der genutzten Datenbank auf dem MariaDB Server](#_Toc533164466)