Plan of Approach - Graduation Internship

Name:	Andres Vivas Rodriguez
Student number:	345155
Institution:	Hanzehogeschool Groningen
Education:	HBO-ICT, Network & Security Engineering
Internship lecturer:	Thies Keulen

Company:	Axians ICS Groningen
Company supervisor:	Peter Eek

Table of Contents

1. Introduction

This report will be known as the plan of approach regarding the internship project proposed by Axians ICS Groningen. The report will consist of defining the current problem, the research aspect , the scope of the project and the professional competences. Let's start by going over the internship assignment.

1.1 The Internship Assignment

Axians ICS Groningen are looking for a solution with which they can implement Authentication, Authorization and Accounting (AAA) on their network equipment within their data center. The data center of Axians ICS Groningen is a complex environment, in which there are strict requirements in place that impact both the security and performance of the network. It is therefore the idea that a proposal is made between different possible solutions, in which they would like to receive advice about the best-fitting solution for their data center.

1.2 Problem Definition

At the moment, there is insufficient central AAA used to manage the network equipment within Axians' network. Axians have their own data center with which there are specific employees who share the same account. This brings 2 potential dangers of sharing accounts.

First, shared accounts have shared passwords. In other words, whoever has access to this shared account has access to the password. This presents numerous password management challenges to overcome. In most cases, this means that the password is written down somewhere. That can be done securely, like in a password manager, but most of the time It is on a sticky note or an Excel spreadsheet. This increases the likelihood that an attacker will get their hands on this password.

The second thing that needs to be addressed when discussing the dangers of shared accounts is nonrepudiation. When you are using a shared account, you cannot prove which user took a particular action. Let’s say, for example, that someone using a shared IT administrator account logged into the VPN at 3 AM and did something malicious or fraudulent. Because 8 people have access to that password, you cannot prove which of those 8 users performed that action. This prevents you from taking action against the individual who performed the malicious activity.

So Axians want someone (an internship student) to advise them of the best possible AAA solution or some other alternative(s) where this problem can be solved. An AAA will not only bring a solution to the current problem but also introduce scalability and central management. There is also a very strict requirement that must be kept in mind when introducing an AAA solution and that is that It must not impact the performance of the current network.

1.3 Practice Oriented Research

This report also contains a section on practice oriented research. The goal of the research is: *How can Axians best realize a central authentication for its network administrators?*

2. Project Scope

The following chapter will be about defining the scope of the project. Project scope is a detailed outline of all aspects of a project, including all related activities, resources, timelines, and deliverables, as well as the project's boundaries. See image below.

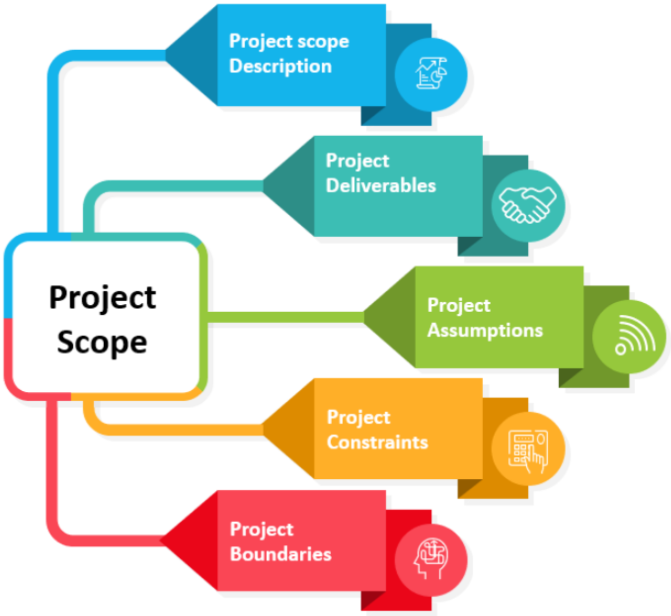


Figure 1: Project scope diagram

The chosen project scope design offers design variations for the project scope cycle, which includes: project scope descriptions, project exclusions, project acceptance criteria, project deliverables, and project assumptions. With this easy to modify and update format, this diagram will help get the project on track with no surprises.

2.1 Project Description

The project is about implementing a new AAA (Authentication, Authorization, Accounting), that can potentially replace the current one that Axians has which is causing them certain issues in different situations.

The project consists of doing research on different AAA protocols to find out which one would be the most beneficial, reliable, secure, etc. for Axians. Beside the technical and security benefits, the chosen AAA solution must also be an financially attractive option.

2.2 Project Deliverables

This is a list of professional product(s) that need to be delivered. The deliverables need to be turned in fully completed in order for the project to be seen as a success.

1.	Proof of Concept (PoC) of the specifically chosen AAA solution
2.	A list of costs of the chosen solution and other alternatives
3.	Documentation of the installation/configuration process of the AAA solution
4.	Fully completed internship report including the professional competences
5.	(Optional) Implement a second AAA server as backup (redundancy), in case the first one crashes or needs to be shutdown.

2.3 Project Assumptions

Assumptions can lead to a deeper understanding of what the project entails, whether the assumptions are right or wrong. There are multiple assumptions that come to mind for the current project. A list of thoughts has been established that are believed to be true yet still need to be confirmed.

1.	There is at least some sort of fully functional AAA service present
2.	There is at least some logging of user activities, maybe through 3rd party programs
3.	There is at least some sort of monitoring tool they use to deal with possible data breaches where accounts get hacked
4.	There are Cisco network devices present, which helps save time due to already having pre-existing knowledge fully understand their function and add specific configuration(s) for the future AAA solution.

2.4 Project Constraints

While there are not many constraints for this project it is important to keep them in mind no matter how few. By ignoring a project's constraints there is a possibility that the project can either be paused or not completed at all. An example in this case would be: If the budget for the project is lower than the needed amount, the project can not be finished and therefore stopped/abandoned.

You can find a list below of the current project constraints:

Constraint	Description
Time Frame	The project needs to be finished within 20 weeks.
Budget	There is no set or an agreed upon budget, only that a solution needs to be presented to the company supervisor with financially attractive options.
Results	The project needs to have a fully functional/financially attractive solution along with a fully documented report in order for it to succeed.
Technical	Due to being an intern, certain systems might be inaccessible or could take time in order to get the permission(s) to work on the project.

2.5 Project Boundaries

While Axians has multiple branches all throughout The Netherlands, the current project is going to be implemented within Groningen, specifically at the branch where I'm currently stationed. The current branch is located at *Zeewinde 5*.

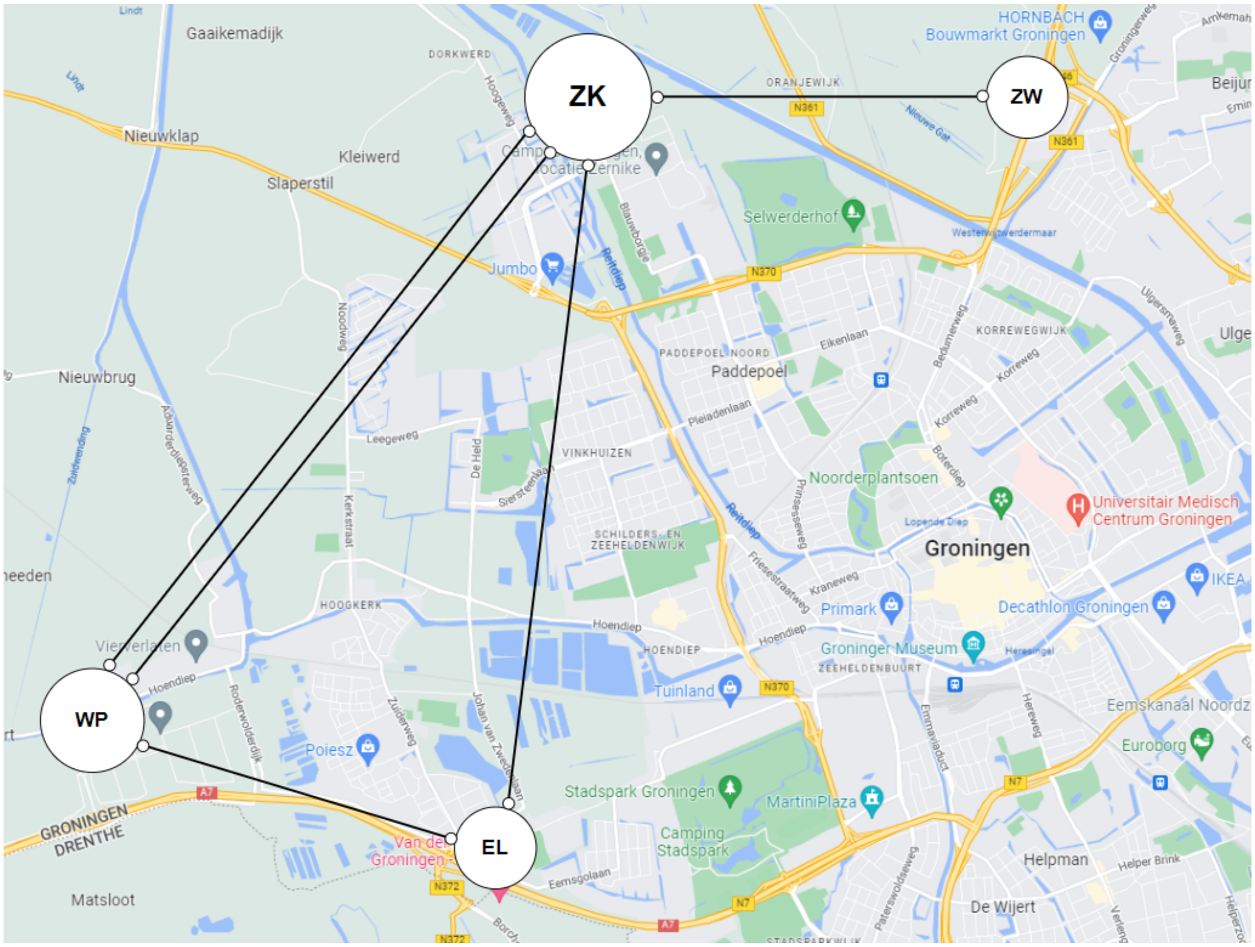


Figure 2: Axians Data Centers

As mentioned in *1.1 The Internship Assignment* , Axians have their own data center(s) which they use to conduct their business. From the image above we can see where these data centers are (based on their abbreviations) located and how they are interconnected. As mentioned previously, the branch where the project will be done is located at Zeewinde, which is indicated by the **ZW** abbreviation. This is where the AAA solution will be implemented.

This is strictly a project between the internship student and Axians, so any 3rd party companies or clients fall outside the scope for this project.

3. Professional Competences

This chapter is going to go over the professional competences for the internship project. The competences are going to cover the Analysis, Design -and Implementation phase of the project. These competences are level 3 HBO competences in accordance with the requirements set by the Hanzehogeschool Groningen. The competences are key in understanding what the situation is, what is going to be done about it and how the solution is going to be implemented.

3.1 Analysis

The analysis-phase is the gathering of information about the current environment and also the current problem which the internship project is based on. In this phase it is the student's job to gather every possible information on the current situation to be able to further plan out what possible solutions there are and how they can be implemented in which the company may benefit from. With that in mind we begin by assessing the current situation.

At the start of the internship the first thing to do was to establish a list of questions (Questionnaire) that can be used to ask different employees within Axians in order to gather more information on the current environment and the issues that may or may not be present.

Here is what was learned:

- Axians currently uses LDAP as an AAA-protocol
- Axians does not have a single sign-on service, but they want to have it
- Axians uses primarily Aruba network devices

3.1.1 LDAP Authentication

Lightweight Directory Access Protocol, or LDAP, is a software protocol that stores and arranges data to make it easily searchable. The data can be any information about organizations, devices, or users stored in directories. LDAP is the protocol used by servers to speak with on-premise directories.The directory is essentially where all the credentials of the users are saved.

The main purpose of LDAP is to serve as a central hub for authentication and authorization. LDAP helps organizations store user credentials (username/password) and then access them later, like when a user is attempting to access an LDAP-enabled application. That user's credentials stored in LDAP authenticate the user. See the image below.

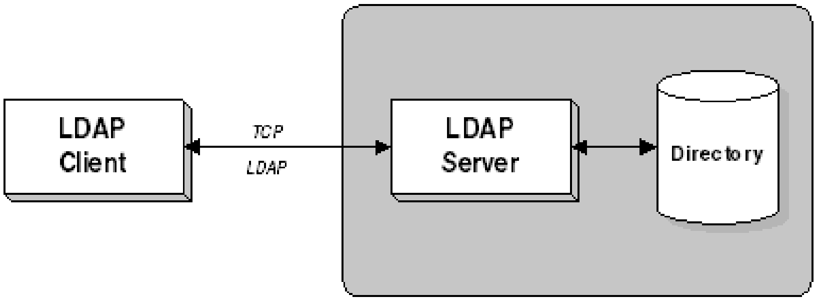


Figure 3: LDAP Overview

LDAP is based on a client-server interaction, as seen on the image above. The client begins a session with the server, called a “binding”. The client presents their user credentials which the server can compare against the directory and authorize access based on that user’s attributes.

The problem that Axians is currently experiencing is that, while LDAP does provide authentication and authorization, it does not do accounting (logging) which makes it hard for network management. If an incident occurs regarding a password leak, how do Axians figure out who was on the account and what was done on said account? This also confirms what was discussed at 1.2 Problem Definition.

3.1.2 Single Sign-On

Another issue that was discovered is that Axians does not currently have a Single Sign-On service. This was found out during an interview with some of the network employees and is something they would like to have when implementing the new AAA solution.

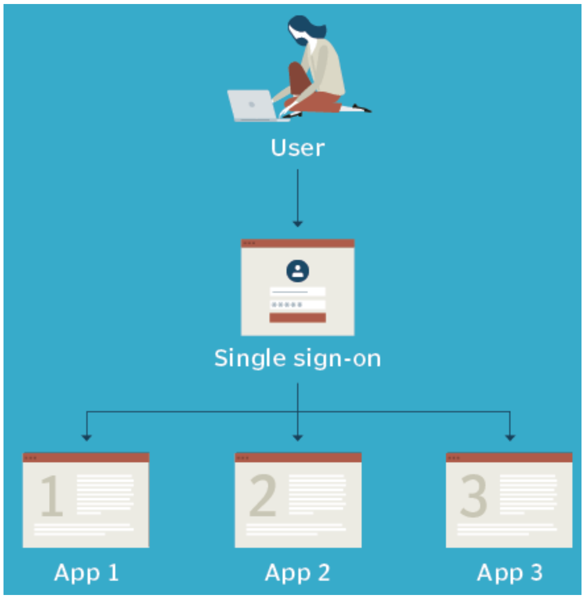


Figure 4: Single Sign-On Overview

Single Sign-on (SSO) is a session and user authentication service that permits a user to use one set of login credentials (see image above). Basically SSO allows users to access all their applications by signing in with 1 account, this eliminates the need for multiple passwords and increases usability, access and productivity.

The problem from not having SSO is that this makes it difficult for network administrators in keeping track of the multiple accounts/passwords needed to access certain devices/applications. For example, because Axians does not have SSO, the network administrators use a local admin account in order to access their network devices. This makes it difficult for centralized user management, it makes it difficult to see which particulair network employee accessed which specific device. This also confirms the “shared accounts" issue which was discussed at 1.2 Problem Definition.

3.1.3 Network Devices

Axians uses multiple different switches within their network infrastructure, one of the main network switches that they use are called **Aruba Switches**. The reason why they use Aruba Switches over the traditional CISCO switches is because Axians are partnered with HPe (Hewlett Packard Enterprise) and HPe have purchased and now own the Aruba network devices.

According to an interview done with an employee, the plan for the future is to replace every switch they currently have/use to Aruba Switches, this of course will take time in order to be fully realized. This is something to keep in mind in order to have a better grasp on how the project will be implemented.

3.2 Design

With the information gathered from the analysis-phase in mind, we now move on to the next phase, the Design. The design-phase is about giving an idea on how the project will be done/implemented later on.

3.2.1 The current idea

The idea is to have a virtual environment built to look like (as close as possible) to the current live environment. The reason for having this “copy” of the live system is to see how the system would act with the new AAA implementation as if it were the actual real environment. Luckily, the virtual environment is a controlled space where if anything goes wrong it does not impact the live systems and can be easily reset or changed when necessary.

The following image is the general idea on the necessary devices/servers needed within the virtual environment. This might change as the project continues.

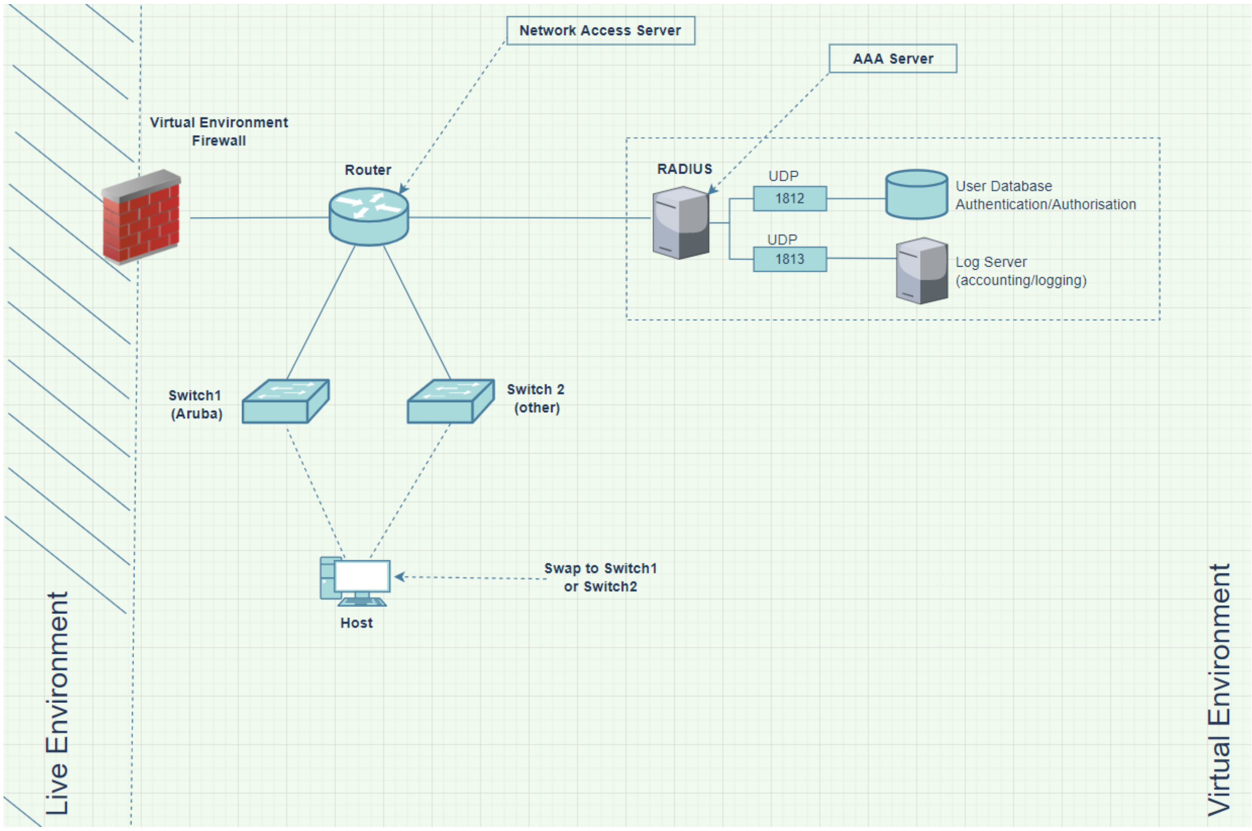

Network Access Server
AAA Server
Virtual Environment Firewall
Router
RADIUS
UDP
1812
UDP
1813
User Database Authentication/Authorisation
Log Server (accounting/logging)
Switch1 (Aruba)
Switch 2 (other)
Swap to Switch1 or Switch2
Host
Live Environment
Virtual Environment

Figure 5: Virtual Environment idea

As you can see, the virtual environment is separated from the live environment specifically by a firewall.

If we begin at the bottom, the “Host” is considered to be a user which either connects to Switch 1 or 2. Switch 1 is an Aruba switch which mentioned before that It is primarily used in Axians’ live environment. Switch 2 is any other switch that Axians may have in their live environment. The reason for needing multiple switches is to ensure that the new AAA implementation works seamlessly no matter the different switches Axians may have and or use.

The router will act as an “Network Access Server” also known as NAS. The NAS is the connection point between the AAA server and the user (host), this device processes access requests from the user to the AAA server and grants permission upon confirming the user’s identity.

Lastly, the main requirement for this whole project, the AAA server. The AAA server will be configured with the chosen AAA (RADIUS in this example). The AAA server then checks the credentials (via port 1812) and other necessities it may need then provides access to the user (Host). The User Database stores the credentials of the users to verify if they are using the right credentials to login with. Lastly, the Log Server is where the logs from the AAA server gets sent to (via port 1813).

* RADIUS was used as an example in the diagram and is not yet certain if it would be the chosen AAA solution in the end.

3.3 Implementation

Thanks to the Design-phase we now have a general idea on how the project will be done and we can move on to the last phase, the implementation. The implementation-phase is about realizing the project and bringing it to a completed state.

As mentioned in the design-phase, there will be a virtual environment set up to look very similar to the live environment, this is where the implementation will take place. However, in order to begin implementing an AAA, we must first establish what the required devices are in order to build this environment.

3.3.1 Hardware Requirements

After discussing with the network department of Axians, It has been brought to my attention that Axians' network consists of different switches. One of the reasons is the different switches currently in place within the system. This means in order to confirm that the AAA solution not only works but also that it can work with not only one switch but multiple switches. Axians

With this in mind, the requirements list can now be established.

Device	**Type/Model**
Work Laptop (Host)	Windows 10 Enterprise
Switch 1	Aruba switch (AOS)
Switch 2	Aruba switch (AOS-CX)
Switch 3	HP Procurve 2600 or above
Switch 4	HP Comware 5
Switch 5	HP Comware 7
Router	Fortigate Router
AAA server	Windows Server 2019 ()
Log server	Linux OS

Depending on the cost and/or availability, the above devices may change. The cost is of course also a very essential factor for Axians and is also seriously considered while looking for the best solution.

3.3.2 The Virtual Environment

The virtual environment will be accessed through a VPN connection using a specific VPN account that was provided by Axians. The VPN account is used to be able to access the server along with an RDP connection. See the image below.

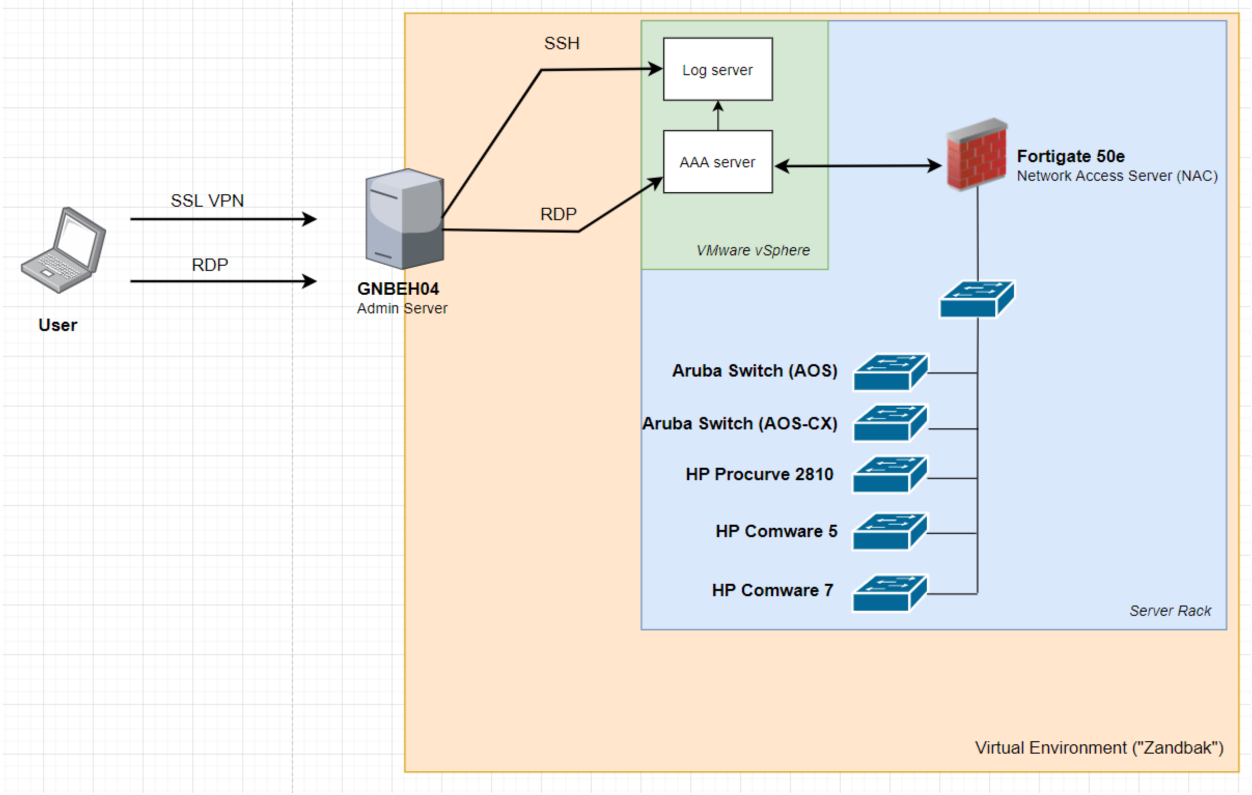


Figure 6: The Virtual Environment

The Admin Server (GNBEH04) is the “gateway” to the virtual environment called “Zandbak”. On the Admin Server you can find a vSphere Client running where the virtual AAA server and the Log server will be made.

The AAA server will run in the beginning on Windows Server 2019 and have RADIUS installed as its AAA protocol. This might change during the internship period.

The Log server will be run on an CentOS 7 Operating system (OS) as they normally use in the Live Environment within Axians.

Lastly, as mentioned before in the design phase, there will be a total of 5 switches that will be used to ensure that the authentication process works on with any of the switches that Axians use within their system. All the switches must go through the Network Access Server (in this case the Fortigate Firewall) which then communicates with the AAA server. The AAA server sends the logging of the authentications to the Log Server.

4. The Project Timeline

The internship period will be 20 weeks, which means that there are 20 weeks in order to finish the internship assignment. A timeline has been established in order to have a good and organized structure for the tasks that need to be completed. The timeline is basically to get a general idea on which tasks are gonna be done and when.

Period	Description
Week 1 - 3	Introduction to the company and gather information on the current situation. Perform a Desk Research on possible solutions to the current problem and document the Plan of Approach with the information gathered.
Week 4 - 5	Establish interviews with multiple employees within Axians. The idea is to not only interview the employees of the network department but other departments as well as they might provide a broader understanding of the current situation, this could prove to be essential to know before implementing the AAA solution. Update Plan of Approach with new discovered information when necessary.
Week 5 - 10	Based on the information of the previous period (week 4-5), this period will be the setup of the testing environment which can be used to experiment with the potential chosen AAA solution without the risk of interfering with the Live systems. Documentation of the process(es) and configurations of this phase must also be done and kept up-to-date.
Week 11 - 20	Within this timespan the AAA solution will be worked on and brought to a fully implemented state. From this point the AAA solution will also be tested in the form of a Proof of Concept (PoC) to see if the solution works as intended. Finalize the internship report and organize the data in a presentable way on Powerpoint. Afterwards, present the internship project to the Internship -and Company Supervisors. (Optional) If possible within the time limit, implement a second AAA to act as a redundancy option.

5. Practice Oriented Research

Research question
How can Axians best realize a central authentication for its network administrators?

Research strategy
In order to be able to answer the research question, an answer to the future sub-questions is needed. To do this a series of ***Interviews*** will be conducted with specific representatives of Axians.

Data collection method(s)
There are a couple of methods that best fit in this situation, they are ***Interviews, Secondary data collection and Documentation***

The *Interviews* will be about conducting one-on-one conversations between the interviewee (employees) and the interviewer. The purpose is to gather as much information as possible in order to build the structure on how the project is to be done and or implemented.

From the information gathered from the conducted interviews, a Secondary data collection will be performed, which is the already available information that has already been collected by someone else (i.e internet publications, wikipedia, etc.). This is to help answer the research question or eventual future sub-questions.

Lastly, *Documentation* is the collection of various data resources and documenting them in a readable manner.

Data analysis methods:
The results of the data collection will be ***qualitatively*** analyzed. What will be analyzed will be the information gathered from the conducted interviews.

Depending on the information gathered from conducting the interviews, there might also be data ***quantitatively*** analyzed.

6. Feedback Moments Agreement

To keep everyone up to date during the internship period and also being one of the requirements from the Hanzehogeschool, there has been a feedback moments table drawn up. This is to have a clear view on the involved parties and how they are gonna be communicated with about any new information or concerns.

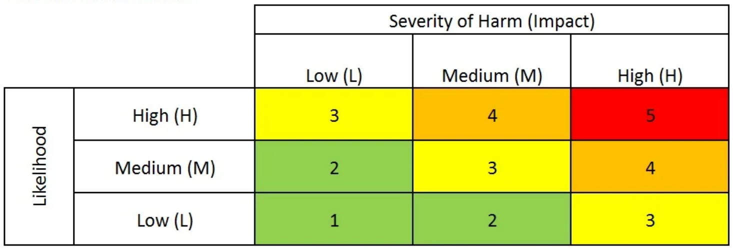
The agreement table:

Name	Role	Agreement
Peter Eek Novak Ciric	Company supervisor Project supervisor	Weekly updates on what will be worked on (Mail, In Person) Contact person for project-related questions (Mail, Phone, In Person)
Thies Keulen	Internship supervisor	“Feedback Moments” meetings every 2 weeks

7. Risk Analysis

This chapter examines the possible hazards that may or may not arise during the execution of the project. By identifying these hazards and taking immediate measures, the risk can be fairly limited. This increases the chance that the project will be successfully completed.

Firstly, we established a matrix of the likelihood of a risk and the severity of the impact.



		Severity of Harm (Impact)		
		Low (L)	Medium (M)	High (H)
Likelihood	High (H)	3	4	5
	Medium (M)	2	3	4
	Low (L)	1	2	3

Figure 7: Risk Assessment Matrix

Secondly, with the table above we can now give the possible risks a numerical value depending on their likelihood and their impact.

#	Risk Description	Likelihood (L)	Impact (I)	Risk (L x I)
1	Sickness	3	1	3
2	Defective network device(s)	2	5	10
3	Lack of knowledge	2	2	4
4	Not able to go to work (physically) due to unknown circumstances	5	1	5
5	Project does not meet the graduation requirements.	2	4	8

Finally, with the risk values in mind we can organize them into a list of priority along with the measures that need to be taken against the specific risk.

Priority	#	Measures Against Risk
1.	2	Contact Company Supervisor immediately and ask for an available replacement
2.	5	Request feedback from the Internship Supervisor and add the missing contents in order to pass
3.	4	Work remotely (from home) by using the provided VPN from the company and keep Company Supervisor informed with anything that comes up
4.	3	Ask for help or guidance from the employees in the network department
5.	1	Work extra hours to make up for lost time