Daily log

Table of contents

Contents

Week 1

1 March 2021

Because it was the first day, I went to the HPE office in Diegem. Here I met Dries (my mentor) and Yannick (my manager). They gave me a laptop, which we then set up properly so that it is ready to be used remotely.

We also went over the assignment together and discussed some details about the internship. We agreed that I will be following along in 2 of their customer projects, alongside the main internship project. This is so that I can get a better view of how they handle their customer projects, and the general way of how work is in HPE.

In the afternoon I started documenting and researching a bit about Windows Admin Center, to get a better understanding of how it works, and why it might be useful in the project.

2 March 2021

Today I started doing some research about Terraform, I'm also working on a case study to learn how to properly work with Terraform in Azure. I need to use Docker to work with Terraform, this should work once my Windows update has completed.

IT support has been contacted for the McAfee problem with the Windows update, they should reach out soon.

Around 9:30 am I joined a call with a customer for who they are using Terraform in a solution. This showed me how Terraform can be used in large-scale production projects.

I've also been documenting some more on my research of Windows Admin Center, and working on the Plan of Action.

A meeting with Bert and Bavo (teammate and team-lead)has been arranged for Monday 8 March 13:30 - 14:00. In this meeting I will learn a bit more about their positions at HPE and about projects they're currently working on.

In the afternoon I have documented some research about HashiCorp Boundary. In a meeting with Dries, I also learned some more about the way projects are initiated in HPE, including the way customers contact them, the different documents that are set up, and all the different steps that take place before a project goes to the delivery phase. Using this theory, I have created a few user stories for the project I will be creating for HPE.

3 March 2021

Planned the startmeeting for my internship with Dries en Mr. Desmyter (mentor at Thomas More) for monday 8 March from 15:00 - 15:30.

Added a few more user stories, and added some more text to the plan of action.

Doing more research on Terraform, and working on the case study. For the case study I was able to install Terraform and configure it to use my Azure subscription. Later I was able to create a resource group and a virtual network interface.

In the afternoon I documented some more research on HashiCorp Boundary. I've also created a case study in which I installed Boundary on my laptop, and created a development environment. In this environment I then created users, groups, roles, and other resources (such as target machines) with a Terraform script.

I've also started working on a document to write down some research about Azure Bastion.

4 March 2021

Added some information about Hewlett Packard Enterprise in the Plan of Action.

Started a research document to learn some more about the Microsoft Cloud Adoption Framework for Azure.

I've also started with a document to further write out user stories. I'm creating this document to understand better why these user stories are important for the end solution. In this document I'm also describing possible technical solutions for the user stories.

At 1pm I joined a sync meeting with a customer of HPE. HPE is designing an Azure cloud architecture for them.

In the afternoon I continued to work on the further documentation of the user stories.

I also had a short meeting with Joren, who is a young graduate at HPE. In this meeting we talked a bit about his position at HPE and what he studied before starting his job here.

---

5 March 2021

Today I started the day by configuring a Ubuntu 20.04 WSL on my HPE laptop. I then installed the "Remote - WSL" extension on my Visual Studio Code. Now I can modify all my files in Visual Studio from a Ubuntu image instead of directly from my Windows operating system.

I also tried out the "Remote - Containers" extension to run all my source code in a Docker container. But this needs WSL version 2.0, my laptop is running version 1.0.

Afterwards I started with another case study for HashiCorp Boundary. In this case study I'm trying to create a HashiCorp Boundary environment from scratch, so not with `boundary dev`, which creates a generated dev environment. I have to create a PostgreSQL database, a controller node and a worker node to create the environment. Then afterwards I'd have to create users, roles, groups, targets, etc.

Currently I've created the controller node, the worker node, and the database in Azure. Initializing the database from the controller node was successful. I'm trying to create a first user and authentication method now, but this is giving errors. I will continue this case study on monday.

Week 2

8 March 2021

Today I started the day with troubleshooting the error I had last friday in the Azure HashiCorp Boundary case study. This took a long time and eventually I had to ask Dries for help. It turned out the boundary service was not running in the background. After fixing this, I was able to authenticate the admin user with the organization.

Wednesday I will further configure the worker node to also have the service running at startup, and create an own organization instead of using the pre-generated resources that I used to test it now.

In the afternoon I also had a meeting with Bert and Bavo. They explained their positions at HPE to me, and we discussed my internship.

At 3 PM Dries and I had a startmeeting with Mr. Desmyter. In this meeting we discussed the guidelines for the upcoming meetings, evaluation, and documents I have to deliver.

---

9 March 2021

Today was the virtual job fair of Thomas More. I went to a few presentations, one explained more information about following a master degree after my current bachelor degree. The other one explained more about life after graduation, everything about jobs and unions.

In the afternoon I visited some company stands at the virtual job fair. Here I learned more about these companies.

---

10 March 2021

I started the day with continuing my work on the HashiCorp Boundary case study. Last time I finished setting up the controller with a generated organization and gaining access to the admin control panel. So today I went on with finishing the configuration for the worker node and then creating my own organization called “Corp Sien”.

In this organization I then created some users, each with roles that declare access rights and some in the read_only group.

In the project scope “Core infrastructure”, I created a few targets, one on port 22, and another one on port 8080. These targets I then connected to a new VM, which will serve as a host.

After some troubleshooting when I couldn’t establish a session for a user to a host, I figured out the SSH private key file was missing on the worker node, which is needed to secure the

connection between the worker and the host. After adding this, the connection was successful and I was able to execute commands on the host remotely through a CLI.

I want to visualize this small architecture in Microsoft Visio, but it's taking a while to update so I might have to do that tomorrow.

Afterwards, I started with a document in which I will explain a potential architecture solution for administrating a hybrid IT environment. In this document I will link user stories to technologies, to explain why we could use these technologies in the solution.

---

11 March 2021

This morning I started with the creation of a visualization of the potential architecture design in Microsoft Visio. In this design I will try to properly visualize what the theoretical implementation would look like. For the actual practical implementation I will have to change a few things, such as using 2 different resource groups in Azure instead of an on-prem and virtual environment.

At 11 am I had a meeting with Dries in which he explained the different Active Directory models to me: on-prem AD, Azure AD, and AD domain services. This meeting really helped me understand the different parts that need to be implemented in the design to create a functioning Active Directory environment.

I continued with documenting this info in my architecture plan, and doing more research.

I also fixed the infrastructure design visualization for the HashiCorp Boundary case study today. So this case study is now fully finished.

At 3:30 pm I had a meeting with Yannick, Dries, and Leslie about the progress I've made so far.

Afterwards I continued working on the "possible architecture" plan. It is not finished yet but the basic information is there, with some more in-depth details on some subjects.

---

12 March 2021

Today I'm continuing with making the visualization of the architecture plan in Visio. Doing this helps me find pieces that are still missing to make the whole architecture work.

I'm also adding more information to the theoretical document of the architecture.

This afternoon there's a Bingo game organized for the entire BeLux, so I also participated in that. I didn't win anything but it was fun.

After the Bingo, I continued with the theoretical document of the architecture.

Week 3

15 March 2021

Today I started the day with fixing a few things in the Visio model of the architecture.

I then joined a two hour meeting with Dries, Timothy VM, and Timothy DL about a project that was made for a customer. In this project they created an entire infrastructure in Azure with the use of Terraform scripts. This was very interesting to see how Terraform can be used to deploy production environments in azure. In this meeting we went over the different files with code to get an overview of how everything works.

Around noon, I started exploring Azure a bit in terms of deploying VMs, configured as Domain Controllers. The goal is to be able to create a VM, in a resource group and virtual network (and subnet), with a simple Terraform script. And then configure this VM as a domain controller with the use of Ansible scripts. Currently I have an error while trying to execute ansible playbooks on the target VM. I will sort this out tomorrow.

---

16 March 2021

Yesterday I tried to promote a VM to a DC with Ansible. But it should be possible to execute Powershell scripts through Terraform on the target VM. This would be easier because I'm already using Terraform to set up the VM in Azure.

After doing some research and getting some explanation from Dries, I managed to get the configuration files working by noon. A terraform script can now create a VM in Azure, and promote this VM to the first DC in a new forest. This simulates an on-premise environment.

Then I continued working more on this testing environment. I created another resourcegroup that simulates a virtual environment. After a lot of troubleshooting, I'm now creating a VPN connection between the two virtual networks. The next step is to install a VM in this virtual environment, which will act as a second DC and perform replication from the on-prem DC.

---

17 March 2021

Today I'm going to try to create the connection between the two virtual networks with VNET peering instead of through a VNET to VNET VPN. This makes it unnecessary to create virtual gateways, and subnets for these gateways.

After this connection was made, I created a new VM in the virtual network, which is promoted to a secondary DC in the previously made domain through the use of Powershell commands.

I had a lot of issues trying to promote the second VM to a Domain Controller. Most of them were because of DNS and connection issues, and another one because of authentication issues. But after a lot of troubleshooting, it was fixed by the end of the day.

---

18 March 2021

Today I started working on a design guide document. The purpose of this document is to explain the different components in the architecture design. It is not meant to provide code or configurations, but it provides an overview of the different components and how they are connected.

In the afternoon I created two visualizations in Microsoft Visio. One of these visualizations is to provide an overview of the different resource groups in the Azure environment, with the corresponding resources in their resource groups.

The other visualization is to provide an overview of the networking infrastructure. This design shows the virtual networks, subnets, NICs, gateways, and connection to the on-premise environment.

---

19 March 2021

Today I continued with the Design Guide document, providing more information around all the components in the architecture design. I then also created a pull request on the repository I keep all the documentation files on, so that Dries can take a look at the design document and give me some feedback.

After this, I started working on the plan of action again. Rewriting a few parts, adding more user stories, and providing more information.

From 1:30 pm until 2:30 pm I joined a sync meeting with a client of HPE. In this meeting they went over changes that were made in the code and how to work with this code.

Afterwards I continued working on the plan of action. I also created the start of a powerpoint presentation for my plan of action presentation next week.

Week 4

22 March 2021

This week I started with making some changes in my design guide and visualizations based on feedback I received from Dries. I then continued with working on my planning for the realization phase of the project. In this planning, I divided the tasks in general lines of

bigger parts (like Active Directory, Windows Admin Center, etc.), and then summed up the tinier tasks that need to happen for every part. For each of these bigger parts I then made an estimation of the time it will take to complete them. I also visualized this planning in the Powerpoint presentation for thursday.

After this planning was done, I continued working on the plan of action, both the text document and the presentation.

I then started organizing my tasks in the DevOps environment.

---

23 March 2021

Today I already started with deploying the basic environment for the project. I created the resources for an on-premises environment, an Azure shared virtual environment, and an Azure spokes environment. These resources include: resource groups, vNETs, subnets, NICs, VMs, Load balancers, availability sets, NSGs, public IPs, and vNET peerings.

This environment has fully been configured with Terraform IaC configuration files. This configuration took me roughly an entire day. I also created a table in the documentation to visualize the naming of the resources.

---

24 March 2021

Today I started with upgrading the configuration for the VMs I configured yesterday, instead of B1s VMs, they will now be B2s VMs. These are faster, but also a bit more expensive.

I then started with “task 2” of the project, the configuration of Active Directory in the environment. First I configured the On-Prem-DC to create a new forest and domain stagesien.com. Then I made sure the DNS settings for NetworkingVNET are set to the IP address of the On-Prem-DC, and configured the DC virtual machine as a second domain controller in the stagesien.com AD domain.

This was again all configured with Terraform IaC configuration files. I had some DNS issues, but these were resolved after troubleshooting for a while.

Afterwards I started with configuring the on-premise AD Connect and Sync agent and the new Azure AD tenant. This is new for me, so I’m testing this out with the GUI first, later on I will code it in Terraform.

---

25 March 2021

This morning I had my first presentation for Thomas More. In this presentation I talked a bit about HPE, the organizational structure, and my project and planning. I received some feedback on this presentation, which I will use to improve it for the second meeting.

Afterwards I continued with configuring the AD Connect server. I figured out a way to automatically download the Azure AD Connect installation client, and launch it. I can't find any Powershell modules to then configure this installation process, so I'm currently doing this manually.

In the afternoon I had a meeting with Dries and Leslie (HR), to discuss the progress I've made so far and what I will do in the following weeks.

---

26 March 2021

Today I'm continuing with configuring Active Directory. I first continued with some troubleshooting for RDP access for users on client PCs, it turned out to be an issue in the local settings of the client, in RDP settings the groups needed to be added.

I then changed some lines in my code to make sure that all VMs are created after the AD domain is initialized, this to make sure that all VMs are added to the domain instead of their local work-groups. This took a while because I had a cycle error in the code, which took a while to figure out.

I've spent some more time trying to automate as much as possible in terms of client and AD configurations, with Terraform and powershell scripting.

Current situation:

1. Manually = Create tenant in Azure AD
2. Automatic - Terraform: configures basic environment, On-Prem-DC is configured as first DC in new forest & domain, second DC replicates, all VMs are clients of domain, AD Connect is downloaded on On-Prem-ADC
3. Manually = Enter information on AD Connect server, and sync will start
4. Automatic - PS script (on-prem-AD.ps1) : AD Tenant suffix is added to domain, Allow_RDP group is created to allow RDP access for users on client PCs, test user is added, Allow_RDP group is added to clients RDP user settings

---

Week 5

29 March 2021

Today I started with configuring Windows Admin Center in high availability mode on the management VMs. To deploy these servers in high availability mode, they need access to a shared virtual disk. Once this virtual disk was created and linked to the VMs, I could initialize and partition it. Then I created a cluster in the Failover Cluster management console. This cluster contains the two VMs and uses the previously created disk as a shared drive.

All of this took longer than expected because there were many issues with the shared disk. The first disk I created was a standard HDD, sharing is only supported on premium SSDs so I had to recreate it. The second disk (premium SSD) turned out to be corrupted before it was even initialized on the VMs. The third disk luckily did work, three times a charm: :-). Then I created the connections to the VMs in the WAC portal.

I then combined powershell scripting parts into one larger powershell file, this will be executed on the ManagementVM0 and will remotely configure aspects of other VMs.

Afterwards I started with the creation of an Azure Bastion, so that I can connect to the VMs through private IPs instead of through the public IPs.

---

30 March 2021

Today I continued with automating the new configurations. First I started with testing out the new bastion and private IP configs. Then I created a new Azure AD tenant to start from the beginning again. I ran the entire Terraform script and fixed a few errors. Then I created a new shared disk in Azure and attached it to the VMs, this can't be done through Terraform sadly, so I'm using the Azure bash CLI for this until I can find a better solution.

Then I spent some time on troubleshooting the powershell script to further configure the VMs, for some reason this ends in an error, but everything is executed as it should, so I will try to sort this out later.

When the PowerShell script was done, all I had to do was fill in the Azure AD tenant configuration, and start sync.

Workflow in steps at this moment:

1. Execute terraform (automated)
2. Create new Azure AD tenant + global admin acc (manually)
3. Create and configure shared disk (manually)
4. Run Powershell scripts (automated)
5. Fill in AD tenant info (manual)

I then ran through this entire workflow again to fix some more errors and make sure it all works properly now (with the exception of the final PowerShell error).

---

31 March 2021

Today I decided to try to implement the solution I have so far in a DevOps pipeline. This will create a better overview of the different tasks there are and put them in an easy to follow order. I had to do some research first before starting on this because I haven't worked with Azure pipelines before.

Currently I have a pipeline that uses the configuration files in my Azure repository. This pipeline will first destroy the terraform environment, it will check with the state file (hosted in an azure storage account) to see what needs to be destroyed, then there is a manual check to see if the working environment is clean after `terraform destroy` was entered.

It will then create the environment based on the terraform configuration files in the repo. When this is successfully done, a manual check is implemented to create the Azure AD tenant and global admin user. Then a shared disk is created in the azure environment and attached to the management VMs, a powershell script will initialize this disk on the VMs and create a volume. I had a few issues with the Powershell scripts because I had removed all public IPs, I have reconfigured these public IPs now with a strict firewall that only allows WinRM access. I will also look into a solution to later remove these public IPs when the configurations on the VMs are finished.

I still have a few issues with these PowerShell scripts but I will continue to troubleshoot them tomorrow.

---

1 April 2021

Today I've been troubleshooting the DevOps pipeline all day. There were some issues with the terraform configuration now that the public IPs are back. Then there were issues with the WinRM connection to the public IPs, which I was able to fix by adding the IPs to the trusted host of the DevOps machine. I tried to do this with SSL certificates first, but this didn't work.

To add these IPs to the trusted hosts file, I need to be able to declare them as pipeline variables. I created output definitions in terraform to output the public IPs to a file, after the `terraform apply` task in DevOps this output file will create pipeline variables from all of these outputs. This configuration took a long time because I encountered many errors

The issue I had all day was with a bug on Azure. When my resources weren't cleaned up in the correct order, Azure would have issues with the full deletion of subnets, vNETs and resource groups. I now have two resource groups with vNETs and subnets inside of them, that cannot be deleted because Azure thinks VMs are still using these resources, the VMs

however are gone. The only way to resolve this is by creating a support ticket on Azure, which I can't do with my subscription.

I'm currently working around this bug by creating different resource group names in the terraform file.

---

2 April 2021

Today I continued with troubleshooting my DevOps pipeline. I configured a script to automate the formatting of the shared drive after it is added to the VMs. Then I properly configured the remote powershell scripts, they now work.

Passing the output of the terraform script to other tasks in the pipeline has been difficult, I've done a lot of research on it but no solution seems to work. So for this moment I'm manually declaring my IP address in other steps of the pipeline, instead of doing this automatically through variables.

In the afternoon I had a meeting with Dries to go over the progress I've made so far. There were some issues with the deployments in the DevOps pipeline, so it didn't all work like it did before. After the meeting I redeployed the pipeline, and it all worked perfectly. I'm not sure what the issue was, but bad luck seems plausible.

Week 6

5 April 2021

Easter monday, holiday. :-)

---

6 April 2021

Today I started the day with researching Active Directory Certification Services. I want to use a certification service to configure a certificate for the Windows Admin Center portal. Doing this will get rid of the untrusted certificate error that keeps popping up at the moment.

After getting an idea of how this role works and what needs to be configured, I started trying several things out. First I installed the AD CS role on a DC, as a standalone root CA, along with the web enrollment service. Then I installed IIS on a managementVM to create a certificate request. This request I then entered in the AD CS web portal, and accepted in the DC. Then I downloaded the certificate file and installed it on the managementVM. The thumbprint of this certificate I entered in the WAC installation .msi. All that was left to do

then was make the certificate file available to a DC through a network share, and import it in the default GPO.

It did take a little while to fully figure out how to properly configure all of this, but by around 2 pm this was done. I used to rest of the day to document the configuration, clean up documentation of last week, and doing some research for a way to implement a password management solution for local admin accounts.

---

7 April 2021

This morning I started with implementing Microsoft LAPS (local admin password solution) in the environment. I had to do some research on how this works first, but by noon it was fully implemented and documented. Because I did everything manually (with a few powershell commands) the past two days, I started working on automating all of this so that it can be implemented in the DevOps pipeline, or at least can be configured quicker in the future.

I managed to automate the majority of the password management solution, but I'm having a few errors with the certificate services. I will further try to fix that tomorrow. I've also changed my terraform configuration so that it doesn't create a bastion and shared disk anymore, so now there is only 1 management VM. I did this because the shared disk and bastion were the biggest costs in my azure subscription and else I will not have enough credits for next month.

---

8 April 2021

Today I finished configuring the automation parts of the certification services. There are still a few configurations that need to be handled manually, but these are now included in manual intervention tasks.

Afterwards I decided it was a good idea to clean up my documentation and clean up the structure of this project. Up until today the installation manual was a collection of code snippets with a few lines of text, this is now changed to a clean overview of all the configuration steps with explanations as to why certain actions need to be done.

I also included a guide in this installation manual that contains the code to set up the same Azure DevOps release pipeline as mine. This makes it easier to implement the same environment in a quick and efficient way.

In the afternoon I also had a meeting with Leslie to talk about the progress and the evaluation of the internship.

---

9 April 2021

Today I started the day with some research on extra security features in Active Directory and Azure AD. After learning about Azure AD Self-Service Password Reset (SSPR), I implemented this in the environment and documented it. Users can now reset their own passwords. Afterwards I looked into some extensions for Windows Admin Center, and installed the Active Directory extension. Now I can create users, groups, etc through the windows admin center interface instead of having to do this directly on a domain controller. This extension only works in google chrome and firefox, so I can't use Microsoft Edge for this. However I'm getting a certificate error for both of these browsers, while my SSL certificate works perfectly fine for Edge. I spent some time in the afternoon trying to find a solution for this, and by the end of the day I managed to get it working. :-)

To use SSPR you need a premium AD subscription, I activated my free 90 days trial for this. This includes many other features, so I've been looking into those as well, such as company branding, etc.

Week 7

12 April 2021

This monday I've started the day with doing some research on auditing and monitoring of an Active Directory environment, and the best practices to implement solutions for this.

Then I configured the VMs in my environment to send their Diagnostic logs to a newly created Diagnostics storage account. I also connected the VMs to a new Log Analytics workspace, because they were still connected to the default workspace that gets created when a VM is made.

In this Log Analytics workspace I can execute queries to check diagnostic data of all the VMs, such as heartbeat data.

I also want to connect my Azure AD tenant to this workspace so that I can execute queries on this too, but since it is a different tenant than my subscriptions default tenant, and there is no subscription in this tenant, I don't think it is possible to connect the Azure AD. I have a meeting with Dries tomorrow, so I will ask him what to do then.

I then spent the majority of the day figuring out the different queries there are, and how to visualize & organize them in workbooks.

---

13 April 2021

This morning I had a meeting with Dries to discuss the progress I've made during the internship. In this meeting he also went over the temporary evaluation he filled out yesterday. I agree with the working points he told me about, so I will work on those to improve towards the future. We also discussed some configurations I still have to make, which I noted down in a list to work on this week.

After this meeting I had lunch, and then I configured an OpenVPN server which is hosted on a Linux VM in Azure. Because I had deleted the Azure Bastion (expensive) I was working with public IP addresses, but this is a huge security risk. So Dries sent me some configuration files with which he created an OpenVPN server in the past. I used parts of code in these files to set up my own OpenVPN server. This code was new to me so it did take me a few hours to figure everything out and get it working.

After this, I removed my public IP addresses from the environment and organized my code to create a pull request on the repository for Dries to review.

---

14 April 2021

This morning I started with reading about the best practices of privileged administration by microsoft. Microsoft has a big guide on these best practices and how to implement them in the IT environment of an organization, so I used this to create a summarization document to gain a better understanding. I've spent around half a day creating this document.

In the afternoon I created a new SSL certificate for the WAC interface, this time on the fully qualified domain name of the server instead of on the IP address. This is more future proof for if the IP address changes in future configurations.

Then I started with implementing the initial configuration of privileged administration, following the document I made earlier today.

---

15 April 2021

Today I continued with the base implementation of privileged administration. For 2 of the configurations I need a certain subscription which I don't have. I will look into getting a trial for this later, and finished configuring the rest of the baseline security measures first.

Afterwards I started with configuring the Security Rapid Modernization Plan (RAMP), which builds on the baseline security measures to improve security in an environment. I also corrected the remarks Dries entered on my pull request. After fixing this, I went back to work on the security RAMP plan.

---

16 April 2021

This morning I continued with the implementation of the security RAMP plan, and finished it before noon. With the exception of the parts where I need a Microsoft defender subscription, I will probably start a trial for this next week (depending on the duration of the trial).

Afterwards I started designing a specific RBAC solution for my lab, with an overview of specific roles with permissions assigned to users. I also included an overview of the policies that are set on some groups and to which workstations they're applied.

I also configured WAC to use Azure AD authentication, this makes it possible to restrict the interface to a set of users. After doing this, I configured RBAC on the servers to further configure who has access to which server in the WAC portal, and what they can do on this server (admin, reader).

However there still is a cookie error when i try to log in with a different account than my global admin account. I'll have to troubleshoot this error some more on Monday.

Week 8

19 April 2021

This morning I started with making some small changes in my Plan of Action, so that I could send it to mister Desmyter. Afterwards I started with setting up the first version of my PowerPoint to present wednesday afternoon. I've included some screenshots of my realizations so far.

At 11 AM I joined a meeting with a client in which Dries helped the client set up a DevOps pipeline for the solution that was previously created for them.

In the afternoon I continued with troubleshooting the cookie error I had last week when I tried to log into WAC with other administrator accounts. After a while I was able to fix it, it turned out the app registration was still tied to the old version (IP address instead of FQDN), so re-directions were causing the cookie authentication errors. I tested the RBAC assignments to the accounts, and they all work now.

Then at the end of the day I changed the scripts I created a few weeks ago to allow RDP and SSPR to fit into the RBAC model.

---

20 April 2021

This morning I started with reading through my design guide document and added some more information as to why certain technologies were chosen, or are important to

implement. Then I read through my installation guide to add information for already existing on-premise environments and production environments. I also configured and documented the Private identity management part that was not fully configured yet.

In the afternoon I changed some parts of the DevOps pipeline to manual tasks. Now that the public IPs are gone, no connection can be made from Azure DevOps to the VMs, so manual tasks describe the configurations that need to happen now.

I also completed a learn module about the Microsoft Cloud adoption framework and tried some more configurations for the Monitor workspace. I also looked a bit more into auditing and found a good guide which I will configure in my lab environment tomorrow.

---

21 April 2021

This morning I started with updating the PowerPoint presentation that I will use this afternoon. Afterwards I used the comments Dries wrote on my pull request to make some changes in my documentation and create a new visualization for the Management cluster.

Then I started implementing and documenting auditing policies in the lab environment. Currently I have a policy for domain controllers and a policy for the other managed devices. The logged events can then be viewed in the WAC portal, however this is a bit unorganized and doesn't give a clean and proper overview. So I'm looking for a better solution for this.

At 4 PM I presented my presentation for Thomas More in which I explained the progress I've made so far and what I still have left to do. I also learned some more about the progress of the other students in their internships.

---

22 April 2021

This morning I started the day with looking into Azure Active Directory Health to provide more logging for the environment. I also did some research on Azure Sentinel, which is a SIEM and thus can serve as a threat detection solution. Sentinel can also combine data from different sources and combine these into workbooks to create visualizations. I was also able to move my azure subscription (including the resources) from my Student Ambassadors tenant to the AD tenant I use in my lab, so now I can integrate Azure AD diagnostics in my log analytics workspace.

At 11:30 am I had a progress update meeting with Dries and Leslie. In this meeting we talked a bit about the evaluation Dries gave me last week. Afterwards I had lunch and then I started working on configuring Azure AD health, and Azure sentinel. I also looked into some different workbooks to have some examples of possible visualizations for the logged data.

---

23 April 2021

This morning when I started up my servers, I received some errors in AD Health Sync, so I spent around an hour troubleshooting these. Afterwards I had a progress update meeting with Dries in which we went over the changes I've made the past week and discussed which features/configurations I can implement next, I made a list summarizing these.

After the meeting I started with implementing Azure AD authentication in the Windows Admin Center portal. Users were previously able to log into this portal with their domain accounts, but did not have to authenticate with Azure AD directly. I thought this configuration was going to be simple, but so far I'm receiving "unauthorized" errors for non-domain admin users, even if these users are in the authorized user settings of the app in Azure AD. I've spent a few hours trying to find a solution for this, but have not found anything that works yet. I will come back to this issue on monday to try again.

I watched this interactive guide that Dries sent me to gain a better understanding of Azure sentinel and automated responses. https://mslearn.cloudguides.com/en-us/guides/Investigate%20security%20incidents%20in%20a%20hybrid%20environment%20with%20Azure%20Sentinel

Then I started documenting this a bit in my installation manual.

I also received a Demo Microsoft 365 E5 organization from Dries, I used this to take a look at the different features this service offers, to later implement my own (trial) subscription in my lab.

Week 9

26 April 2021

This week I decided to start with securing the WinRM connections to my machines in the environment. I've configured my machines with SSL certificates to use WinRM over HTTPS (5986) instead of over HTTP (5985). So I also deleted the previously used HTTP listener.

Then I limited the allowed incoming connections to this port to the IP address of my ManagementVM. Users will first have to authenticate towards my ManagementVM before being able to use Remote PowerShell on other servers.

I also changed my previous Terraform configurations to not include port 5985 in the Network Security Group configurations anymore.

Then I secured the RDP ports of the machines to only allow incoming connections from ManagementVM0. I accidentally locked myself out of my client with this, after trying to fix it from the Azure portal I only made it worse so I recreated the VM (luckily it was only the client). I will have to make sure that everything is configured right tomorrow.

27 April 2021

Today I continued with troubleshooting my newly created Client. I had to do a few configurations to make sure that it is up to date again.

The RDP connections of all machines (except my client) are now limited to only allow incoming connections from the Management VM. Just like with WinRM, users will first have to authenticate with the ManagementVM before being able to RDP to other machines in the environment.

Afterwards I looked into the issue I had friday again, where some users could not access the WAC portal even though the configurations listed them as authorized users. I still couldn't figure this issue out so I asked Dries for help, we have planned a meeting for tomorrow to troubleshoot the issue.

In the meantime I started configuring some Sentinel workbooks to only display useful data.

28 April 2021

This morning I continued with the configuration of the Sentinel workbooks. I created queries that show the audit events of high level admins (enterprise, domain), which I will later also configure alerts on.

Then I had my call with Dries to go over the WAC Azure AD authentication issue, we went over the different configurations and tested a few things. I ended up re-installing the WAC gateway and re-registering the Azure App, but this didn't resolve the error. I decided to leave the error as it is right now and focus on my other tasks.

The rest of the day I used to configure Alert rule queries in case specific events happen. I created queries to create alerts in case an Emergency BreakGlass account logs in, a privileged user logs in, a critical system is down, and when a large volume of traffic is detected to an uncommon domain.

I also created two Azure Sentinel workbooks that display the events of privileged user accounts, and servers in the environment. These workbooks make it easy to analyze/monitor events.

29 April 2021

This morning I started with testing and troubleshooting some of the alerts I created yesterday. I apparently configured my alerts in the wrong place (Azure Alerts) for them to be integrated with Azure Sentinel. But this was easily fixed by copying the queries to the configuration in the right place (Azure Sentinel Analytics).

When these alerts were configured in the right place I was able to configure incident creation rules on these queries. After a query detects a result, an incident is created. I spent some time testing if logging in with an emergency breakglass account did create an incident like it is supposed to, it did not in the beginning but after some troubleshooting it worked.

Afterwards I configured an automation playbook that will get executed when one of the incidents is triggered (Emergency BreakGlass user login). This playbook will retrieve the user account from the query, and will then disable it. I want to add a step that first sends an email with 2 buttons, one for disabling the account and another one for ignoring the incident. But I'm still getting an authorization error in the last step of the playbook where it disables the user account. So I'll have to work on this some more tomorrow.

---

30 April 2021

Today I figured out what was wrong with the permissions of the Logic app playbook, I managed to give it the right permissions to update regular user accounts, but not global administrators. Because of this I've changed my playbook to send an email when an EmergencyBreakGlass account logs in, instead of automatically disabling it. When an administrator receives this email they have to click on a link that's provided in the email to manually disable the account.

I've also created another playbook that will be used as an automated response for the "privileged users login". This playbook sends an email to an administrator with 2 options: Approve and Reject. If the admin chooses Approve, the user account in question will automatically be disabled, if the admin chooses Reject, the incident will be ignored and closed.

Then I created a last playbook for the incidents that are triggered when a critical system goes offline. In this playbook the VM will be brought back online automatically after it has not send any heartbeat events in 5 minutes. If a machine needs to go offline for maintenance, the incident creation rule can simply be disabled.

These playbooks all came with their own difficulties to configure, so it did take a while to get all of this done. Monday I will continue with adding some extra functionalities to them.

Week 10

3 May 2021

Today I finished configuring my critical system downtime playbook, in which I added a step to first send an email to an administrator to check if the system has to be brought back online. I also finished configuring my last analytics incident creation rule to check for suspiciously large volumes of traffic to uncommon domains.

Then I read over my documentation to add some more explanation in certain parts, for example about the WAC AD authentication.

In the afternoon I added some configuration steps to deploy RBAC on WAC servers automatically with a script instead of manually configuring this per server. I also changed my DevOps pipeline, it now includes manual instructions instead of remote powershell scripts that don't work because of the lack of public IP addresses.

Then I configured and documented the final steps in the privileged access implementation part which I needed a subscription for.

---

4 May 2021

This morning I started with documenting and configuring backups in my lab environment. This was fairly straight-forward and did not take too long to configure.

During the rest of the day I cleaned up my Terraform and PowerShell scripts. I also read through my Design guide to fix a few typos, and add some more text. I made a starters page on my portfolio to host my internship documents on.

Then I added the Terraform and PowerShell files to a private GitHub repo, to link on my portfolio. I also added the design guide to my portfolio after transforming this from markdown to docx, making some edits, and transforming it to pdf.

---

5 May 2021

This morning I uploaded a PDF format of the Plan of Action to my (private) portfolio. I will make this portfolio public when all the documents are reviewed to make sure nothing confidential is in these documents.

Then I had a meeting with Dries to go over the configurations I made in Azure Sentinel, we also discussed how I will present my internship documents on my portfolio. He sent me a template that I could use to make the formatting of my documents more HPE-like, and thus make it easier to re-use parts of the documents in the future.

For the rest of the morning and a part of the afternoon I made some basic changes to my documents, using the template I received earlier.

In the afternoon I started creating a user-manual document which will serve as a guide for the different types of users that can exist in the environment, like regular users and the different types of administrators.

---

6 May 2021

This morning I added some more text to the user manual. Afterwards I started with configuring another incident creation rule and automation playbook to send emails when an error is detected on a critical system. I wanted to add this query and automated response to the "critical system downtime" rule, but combining these queries didn't seem to work very well.

When I was testing this playbook, I noticed some SSL errors in my connection through WAC to the servers. I tried to fix this, and eventually it was (partly) fixed but I am not sure how, so I think the errors might come back.

Eventually I got the playbook to work, but the information in the email that gets sent out is in json format instead of in normal readable text. I tried to fix this for a while, but have not found a good solution yet.

I also had a meeting with Leslie and Dries in the afternoon to talk about the progress of the internship and what's still left to do on my planning.

---

7 May 2021

Today I decided to focus on my documentation since the majority of my configurations are already done, with a bit of fine-tuning left to do next week. I started with converting my installation-manual from markdown to docx, to then apply an HPE template to the file. I spent the entire morning adjusting the styles, tables, images and overall look of the document to make sure that it is properly readable and organized, and fits the style HPE uses.

In the afternoon I focussed on the content of this document. I read through everything, fixed typos, added more information, and removed wrong/redundant information. It is a 70 page document filled with information currently, so this took me a long time.

At the end of the day I also managed to fix the json format in the email step of the critical systems errors playbook. It is now in a more readable text format.

Week 11

10 May 2021

This morning I started with transforming my design guide and plan of action to a proper layout using the HPE word template. I then read through the documents to change some typos, and add some extra information. They are not done yet, but it's a first draft.

The rest of the afternoon I used to create the beginning of a PowerPoint presentation which I will use to present a demo to some employees of HPE in the final week of my internship.

---

11 May 2021

In the morning I made some changes in my environment that I had not fixed yet. Like creating proper emergency access accounts (cloud accounts), instead os directory synced emergency accounts. I also joined a meeting with a client at 10am.

After this meeting I corrected some text in my installation manual, and added some more information based on Dries' comments.

In the afternoon I started with some research on Network security groups, to fully finish the configurations of the security rules in my Azure environment and make them as strict and secure as possible. I've set a baseline of rules now, which I will finish tomorrow. I also replaced the passwords used in my Terraform configuration with a secret which is stored in an Azure keyvault.

---

12 May 2021

Today I documented the rest of my Network Security Group configurations, I will ask Dries for feedback on them before implementing them. Only the necessary communication is allowed through all the machines now, without limiting any services. For the rest of the morning I worked a bit more on my user manual, adding some more information for certain admin types.

The rest of the day I worked on my portfolio site to fully prepare it for the hosting of my internship documents.

---

13 May 2021

Holiday.

---

14 May 2021

Bridge day.

Week 12

17 May 2021

This week I started with proof-reading all my documents again, to prepare them to be reviewed by Dries. I added more information too where necessary. They are big documents so this took me the majority of the day.

I also changed a few manual configurations in the installation-manual to automatic scripts.

Then I fixed a few mistakes in my Network Security Groups overview, which I also created a pull request for to be reviewed.

---

18 May 2021

This morning I started configuring the windows Admin Center servers to run in high availability mode again. This costs more, but it will provide a better view for my demo of next week. I had a lot of issues with the installation here, first it were AD issues where my permissions weren't configured properly, and later I had issues with the SSL certificate (each re-install took at least 20 minutes). At the end of the day I was finally able to fix it for Firefox, but in Chrome and Edge I'm still getting an SSL error.

I changed a part in my documentation to include code to update SSL certificates in High Availability mode configurations for Windows Admin Center. I also changed the firewall configurations for WinRM and RDP for each server to allow incoming connections from the entire cluster, instead of from one ManagementVM only.

---

19 May 2021

Today I added a table to my design guide that includes the network flows that are necessary for the servers to properly communicate with each other. Afterwards I worked on my PowerPoint and plan for my demo of next week, the majority of it is prepared now.

In the afternoon I also worked on my user-manual, I added some screenshots and some more links to find extra information.

---

20 May 2021

Today I implemented the Network security rules which I made a plan for a few days ago. Then I updated my demo presentation a bit and rehearsed it a couple of times. I also implemented an Azure bastion again so that I can use this instead of the OpenVPN server in my demo. I had a few errors with this Bastion but that was fixed rather quickly.

In the afternoon I had a meeting with Dries and Leslie in which I briefly showed them the slides and screens I will be showing during the demo, on which they gave me feedback. After this meeting I made my internship documents and code available on my portfolio, after updating some links in my documents.

---

21 May 2021

This morning I made a few small changes in my PowerPoint and architecture model based on the feedback I received from Leslie and Dries yesterday. Then I started writing the code to implement the previously configured network security group rules with terraform.

All my documents are finished now (except the reflection document), so they are made available on my portfolio and in the Azure DevOps repository. I also re-organized this repository to make it easier to navigate.

Week 13

24 May 2021

Holiday.

---

25 May 2021

This morning I went through the different aspects of my demo again to make sure that everything worked properly. At 9:30 am I also joined a meeting with a customer to discuss an update for a project HPE is developing for them.

Then at 1 pm it was time to present my demo. This went well, I received some good feedback, and it was fun to present the project I've been working on these past months to other people.

---

26 May 2021

Today I cleaned up the Azure DevOps repository that contains all my internship and research files to make it more organized and easier to find the correct files. I also started working on my reflection document.

My project is finished but I have some time left, so I decided to do some more research on HashiCorp Boundary, which had a new update a few weeks ago. This update makes authentication with Azure AD possible, which is pretty interesting.

27 May 2021

This morning Dries filled out my final evaluation and presented this to me to provide me with some feedback. Afterwards I made some final changes to my portfolio website, and cleaned up the files on my laptop. I also made sure to send the files I still need (like my presentations and logs) to my student email address.

Then in the afternoon I joined one last meeting with a client of HPE.

28 May 2021

Today is the last day of my internship. At 10 am I brought back my laptop to the office in Brussels, and had a final meeting with Dries and my manager Frederic.