3-2: Demonstrate your new working password policy

Before applying our group policy, we are unable to change our password to a password that has been used before 24 passwords have been used before it, to demonstrate this we can attempt to change our password and see the error we get.
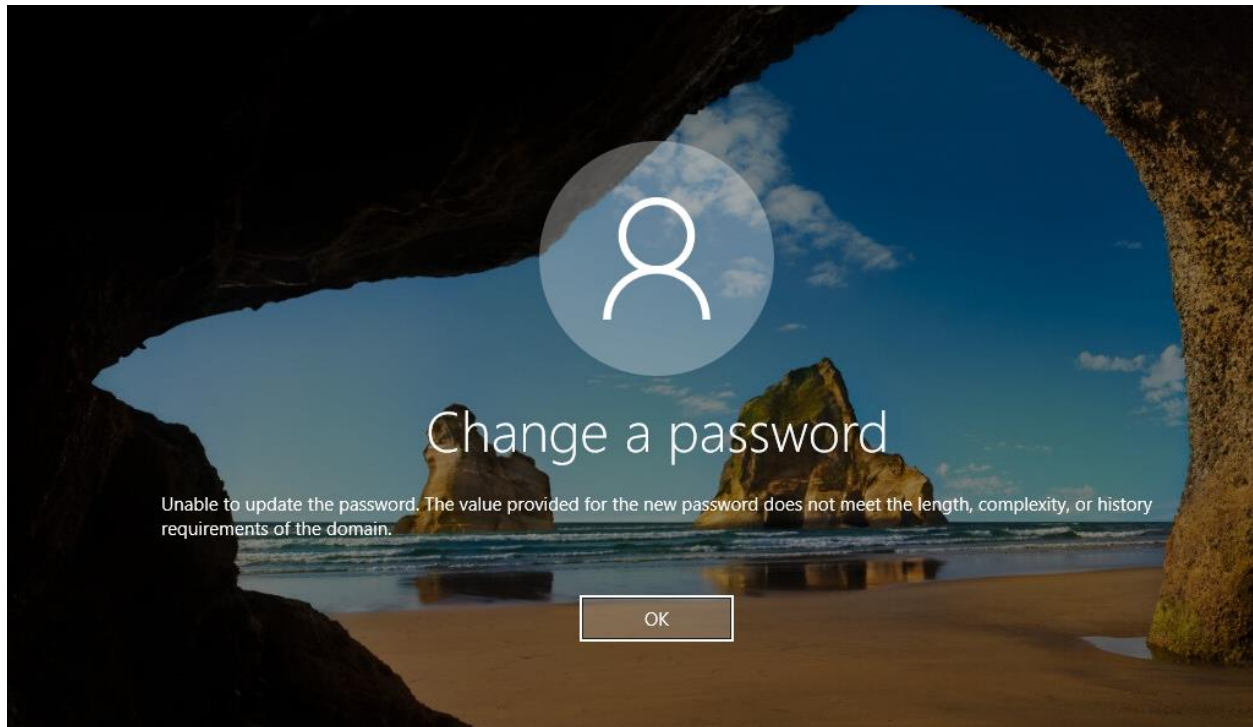

Figure 1: Failed password change because of group policy

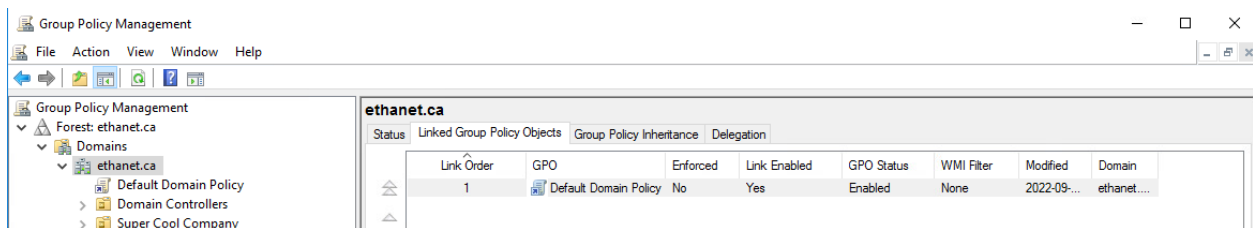We can see our linked policies below.

Figure 2: Current linked GPOs

In the figure below, we have our new password policy that has been linked to the domain
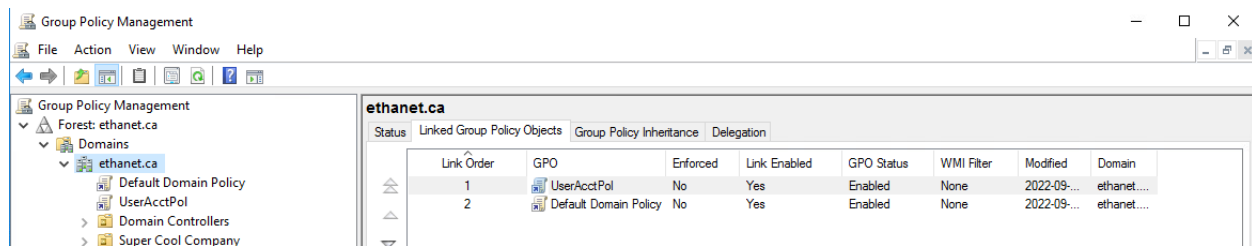

Figure 3: Linked 'UserAcctPol' Policy in place

When we now try to change our password to our old password before applying 24 new passwords before it, we are given a successful change.
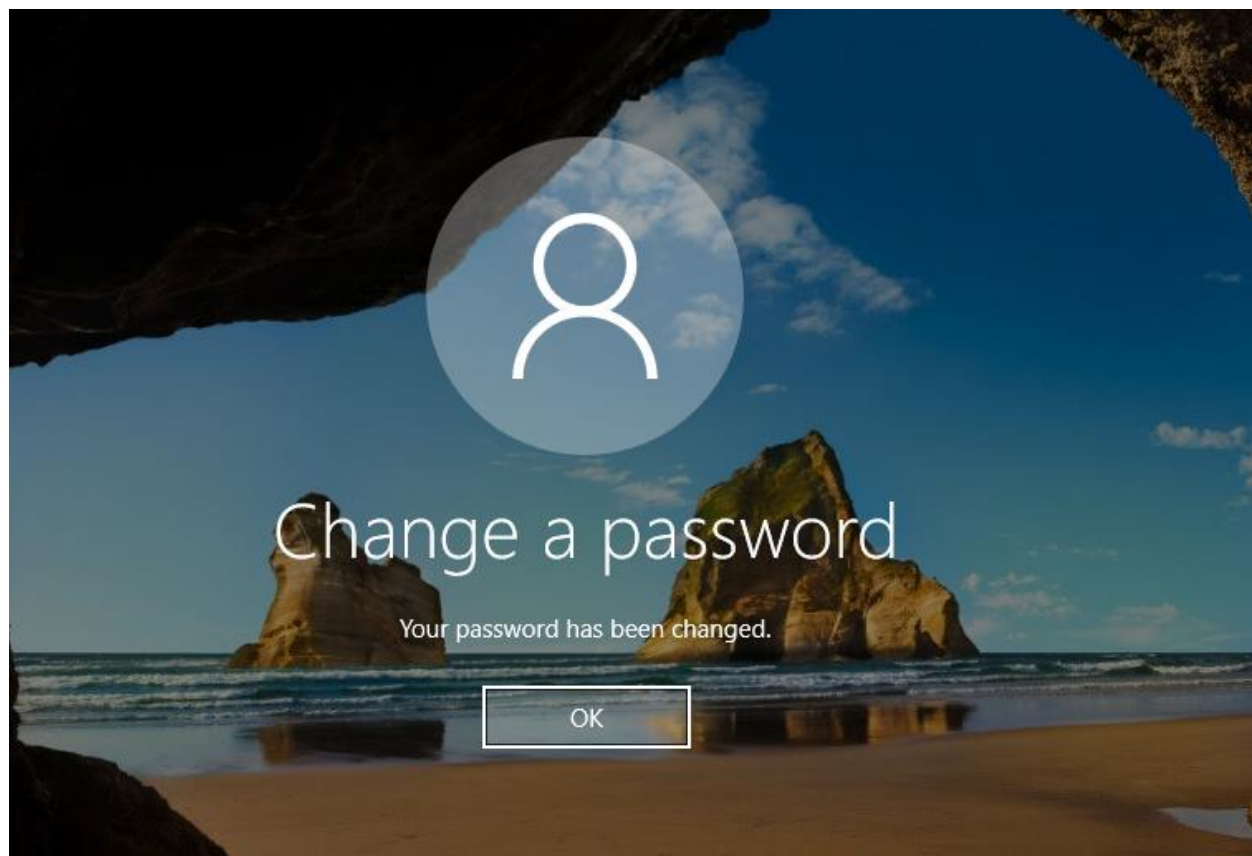

Figure 4: Successful password change

3-4: Demonstrate your account lockout policy

After setting my user lockout policy on my domain, we can see that after 2 unsuccessful attempts to log in, the domain refuses to allow us to log into the account.
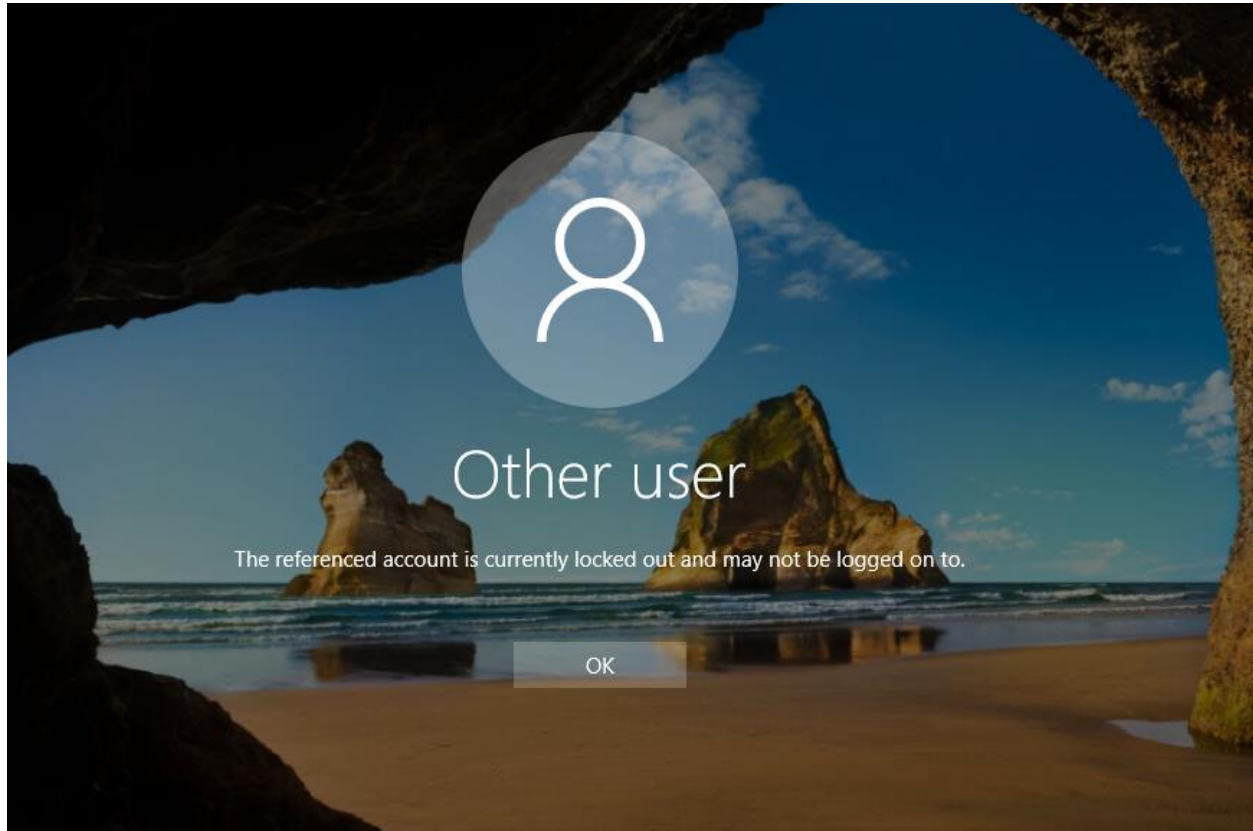

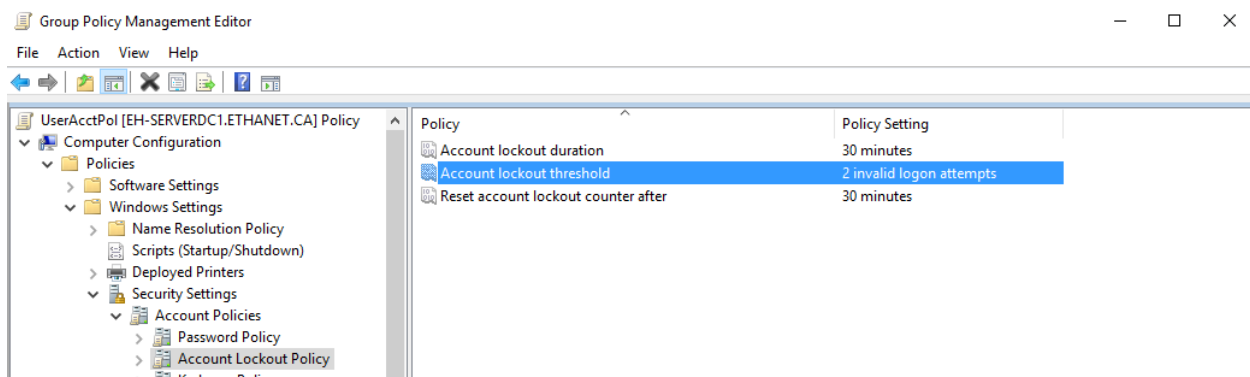*Figure 5: GPO locking testuser out of their account*

Figure 6: UserAcctPol Account Lockout policies

The figure above demonstrates the policies and their settings that we have in place and currently activated.

3-5: Demonstrate the end results of this activity

For this activity, we need to make PSO and add a test user to the PSO, the PSO itself will have a password that is shorter than the domain default of 7 or more characters, here in the figure below we can see that we have a shorter than 7-character password
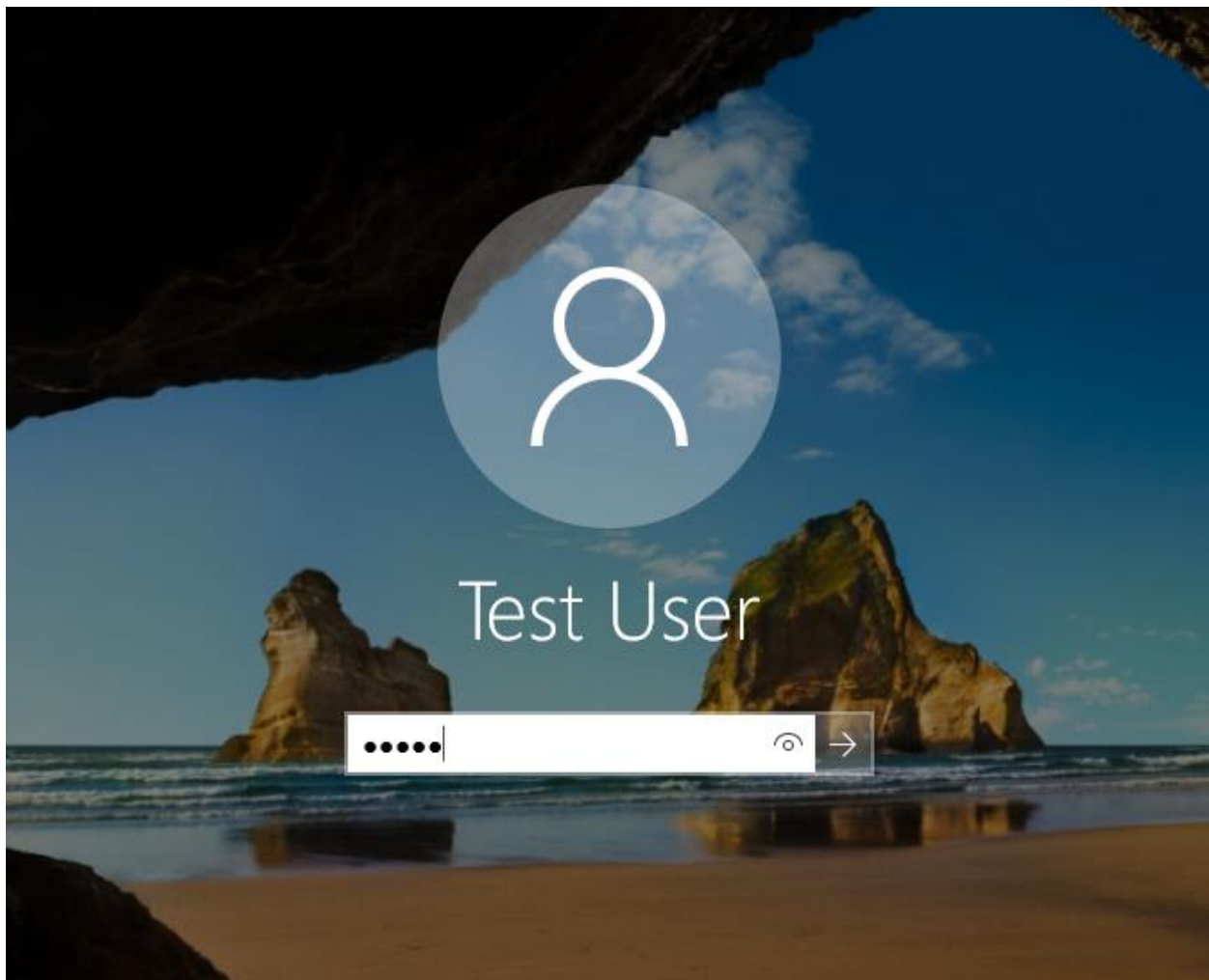

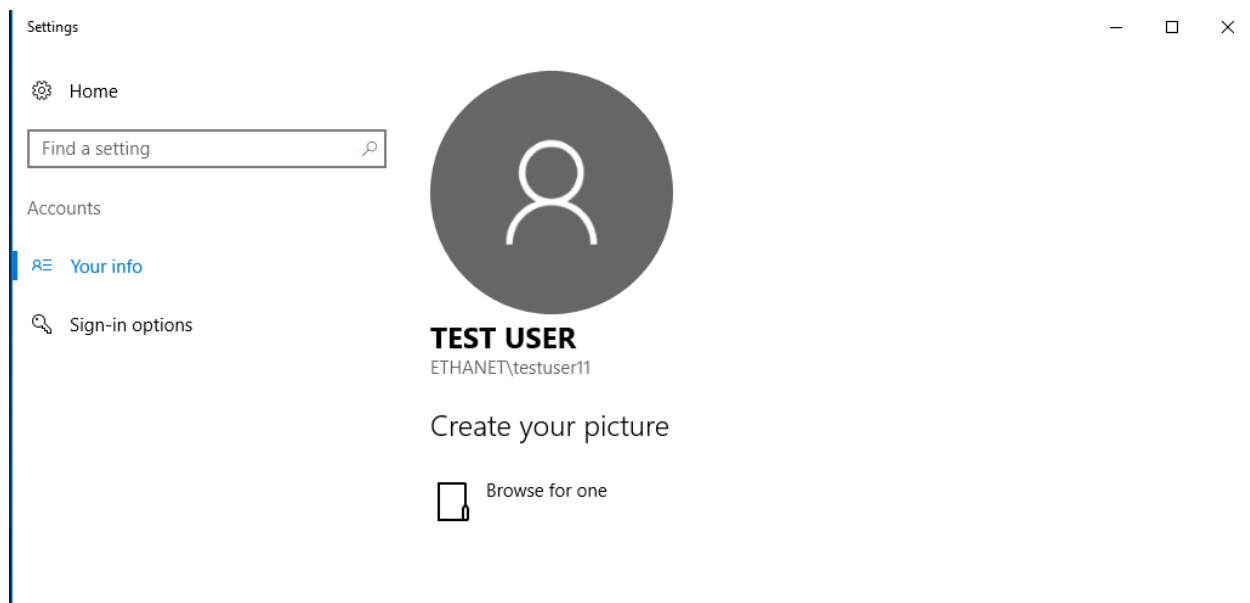*Figure 7: Logging into test user with a short password*

Figure 8: Test User has been signed in

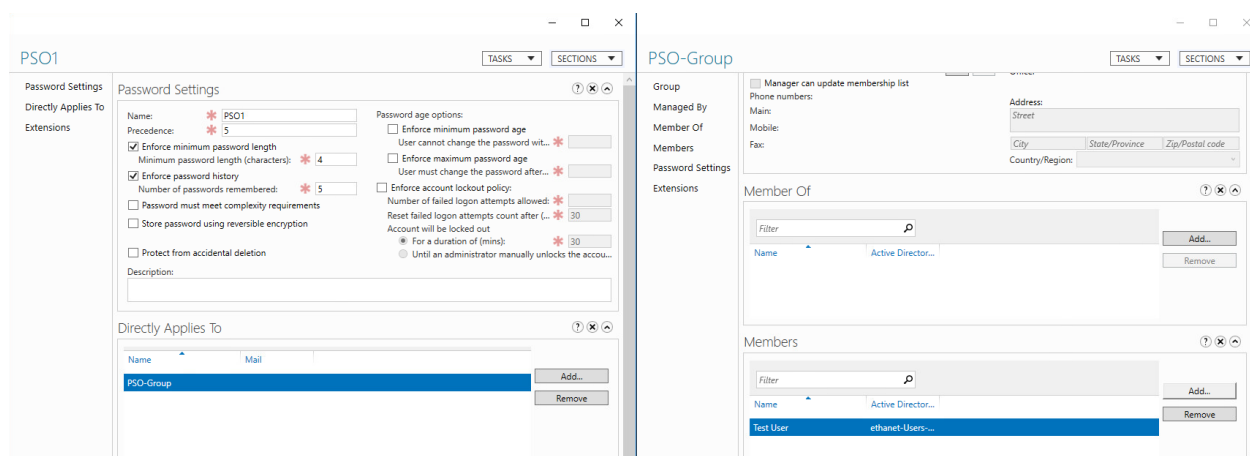This is possible because of the test user being assigned to the PSO group

Figure 9: PSO1 and the PSO-Group

Active Directory Design:

The figure below is an AD layout example for the eLoans & Child Services company
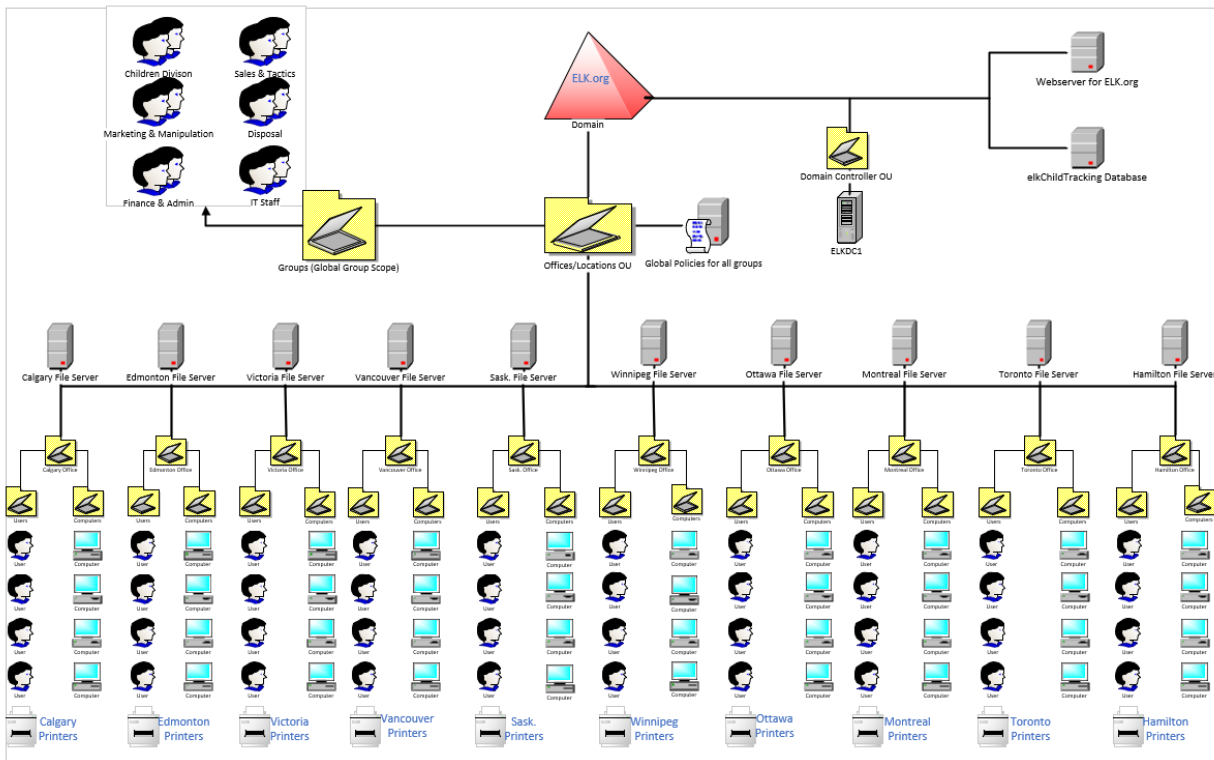

Figure 10: eLoans & Child Services Directory layout

The Primary Domain name for the eLoans and Kids company was ELK.local, some of the policies that we had in place for the company were the following:

Username Convention: FirstNameLastNameInitial.Department (ex. EthanH.Sales)

Password Requirements: 10+ Characters, Numbers/Special Characters included -Apply at Office OU

Account Lockout Policies: 3 attempts, after the 3rd attempt you are locked out for 15 minutes.

These policies are global and applied at the Office/Locations OU level, this allows all the locations on the domain to have the same settings for naming and password conventions. Groups will be handled on a Global Group Scope level as we can apply appropriate settings to each group and each user can be assigned to the appropriate group with permissions across each office. Printers are handled locally at each office and network managed on site. We will also supply a domain controller to control all things

related to the domain and have a database for tracking all children set out by the company, as well as a webserver for hosting the webpage for our company.

Each office will also get their own file server to access and use for remote file services, these can be internally managed, and shares can be created and managed by IT staff, who will create shares for each individual department.

Security Policies will be applied locally at each office (No Room to include) however users will be restricted to accessing most features such as control panel and other features due to the secure nature of our company. Trusted IT staff will be the only exception to these rules.

Conclusion

This project has shown that I think its difficult for me to come up with active directory design in my current state. I am sure that I missed various things that are needed for a well functioning active directory, however I think it was a good project and made me think about the various things that are needed to make a domain or business function.

References

MCSA Guide to Identity with Windows Server® 2016, Exam 70-742

Types of Active Directory Groups & Scopes, Imanami https://www.imanami.com/ad-group-types-universal-groups-global-groups-domain-local-groups/