**Week 5 Assigment- create group policies**

Prof. Kristen Macdonald

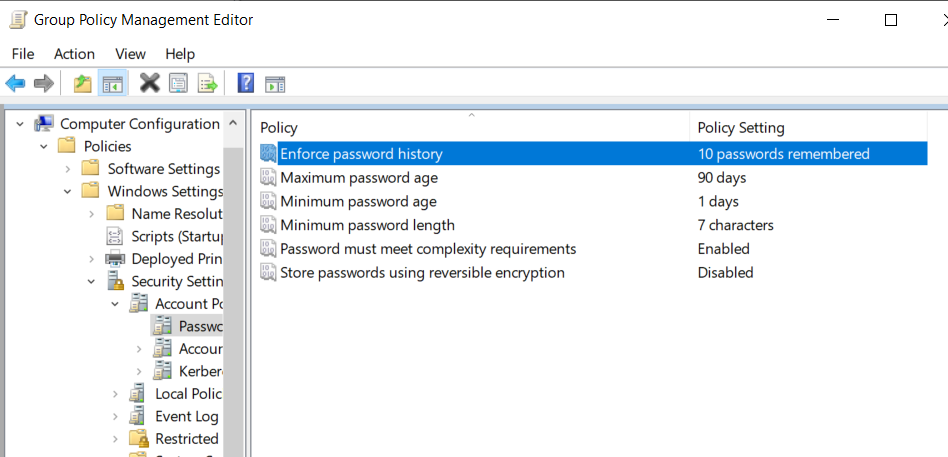
Group No. 4

**Week 4 Assignment: Group Policies**

Create group policy objects in your lab environment, and write a brief report explaining Kerberos policy settings and group policy processing settings. Submit one report per group.

Part 1: Group Policy

1. Adjust the password policy in the Default Domain policy
   1. Include a screenshot of the settings



* 1. Explain your reasoning for each of the settings you chose.

>> **Password history**: The password history is chosen 10 for our company so that our employees don’t use the same last 10 passwords and trying to keep the systems more secure.

**Maximum Password age** is kept as 90 days so that changing passwords every 30 days doesn’t prove as an overhead and the security is maintained by changing the passwords in a 3-month period. Also, if the password change frequency is higher then people might tend to keep simple passwords leaving the systems more vulnerable.

**Minimum password age**: So that individuals can change their passwords at least after a day so that they don’t bypass the password history policy.

**Minimum password length**:

The password must meet the complexity is enabled because sometimes individuals try to keep simple passwords to make it easier for them but puts the systems at risk because they can be easier to crack.

**Password must meet complexity requirements:** The requirement of having a complex password makes it mandatory for the employees\individuals to use a complex password which will reduce the chances of password getting hacked.

**Stores password using reversible encryption**: This setting is disabled to ensure that the encrypted passwords cannot be decrypted. If this setting is enabled an attacker can who has broken the encryption can use the compromised account to sign into the network resources.

1. Create a folder on the file server
   1. Create a group policy that will share this folder with a specific department
   2. Include a screenshot of both your folder and the created policy

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Users in IT security:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. Create a Password Settings Object
   1. Include a screenshot of your PSO.

A screenshot of a computer

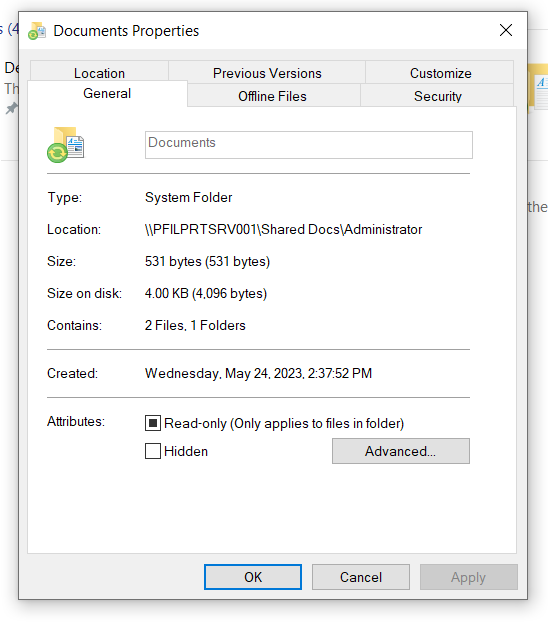
Description automatically generated with medium confidence

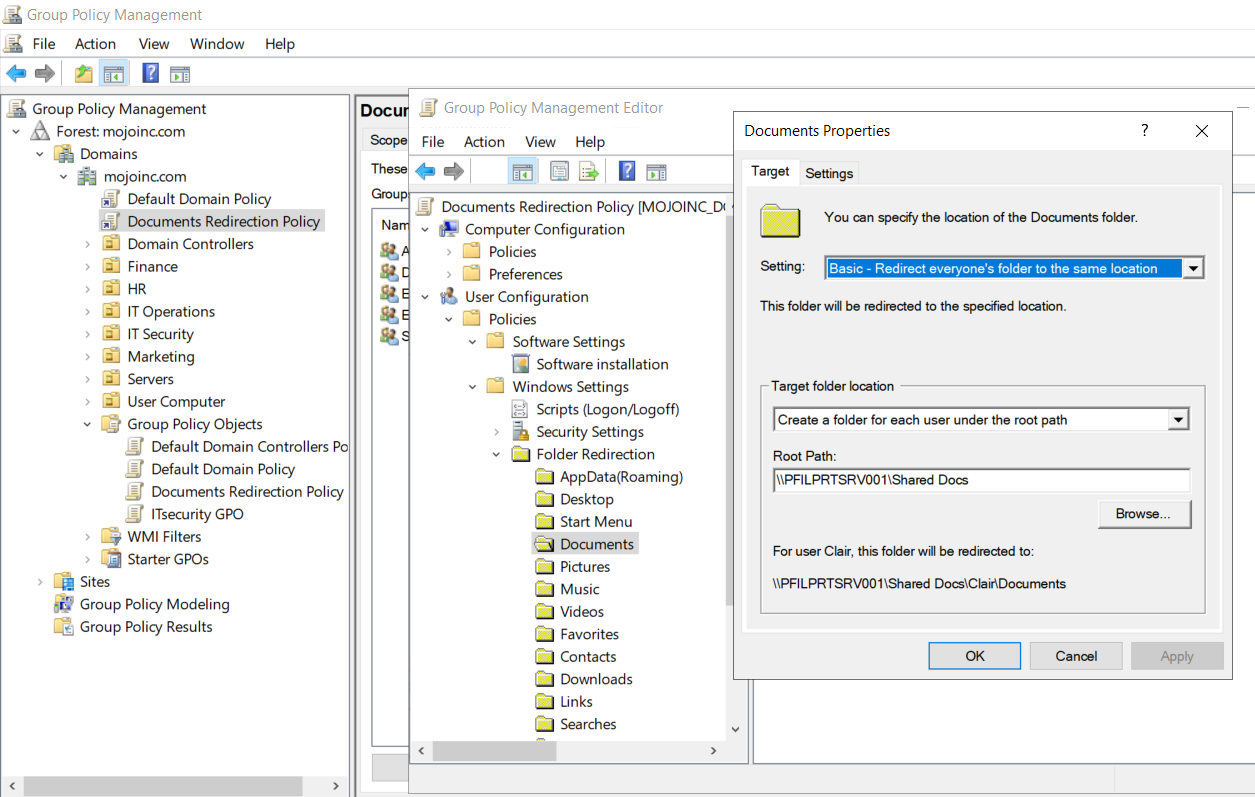
* 1. How is a password settings object different from a password settings policy?

>> A fine grained password policy can be used to apply different password and account policies to different users in the same domain, this is achieved by creating a PSO. A PSO (password setting object) is a policy stored in the Active Directory which holds all the settings of that password policy. These PSO’s can be associated to the security groups whom an administrator wants to follow those password settings depending on their roles and responsibilities.

A PSO has the same settings as a group policy object (GPO), it enables the administrator to give different account settings to different users. Each PSO is assigned a precedence number and the PSO with the lowest precedence takes the priority over the other precedence index.

1. Create a policy to redirect the user’s Documents folder to a shared folder directory on the file server.
   1. Include a screenshot showing your policy and its settings.
   2. Create a folder on the User’s PC and ensure that it is populated in the dedicated File Server directory.





1. Create a user account to be used as a service account
   1. Assign the user account and SPN.
   2. Take a screenshot of the account, including the delegation tab.

A picture containing text, screenshot, font

Description automatically generated

A screenshot of a computer

Description automatically generated

Part 2: Kerberos

In your own words, write a summary explaining Kerberos. Include:

1. The components of Kerberos and what each one does:

>> Kerberos is a network authentication protocol that is used for securing communications over the network. Kerberos offers tickets to the communicating parties and helps to authenticate them to have secure communication. It has components:

* Client: helps in the service request for communication with the user
* Server: The server hosts each and every necessary service which are essential for the user.
* Key distribution center (KDC): It is an integral part with logical components It is a database that holds the keys used for authentication purposes.
* Ticketing granting server (TGS): it is an authentication token used for requesting a service that issues access tickets for a certain resource to join a domain or server.
* Authentication server (AS): authenticate the user and the server and assign ticket via ticket granting ticket (TGT)

1. Each of the available Kerberos Policy Settings that can be enforced through Group Policy and what they do

>>

* Enforce User Logon Restrictions – This policy setting makes sure that Kerberos verifies users' login activity and ticket credentials.
* Maximum Lifetime for Service Ticket – The Kerberos service ticket's validity period (in hours) is determined by this policy setting.
* Maximum Lifetime for User Ticket- The Kerberos user ticket's validity period (in hours) is determined by this policy setting.
* Maximum Lifetime for User Ticket Renewal- This policy setting establishes how long a user must renew a ticket once it has been issued. (in days)
* Maximum Tolerance for Computer Clock Synchronization-The maximum time discrepancy between the clock and the domain/server is specified in this policy setting. (In minutes)

Part 3: Group Policy Processing

1. In your own words, explain:
   1. What the SYSVOL share is on a Domain Controller.

>> It is an acronym for System Volume (SYSVOL), a shared folder located on a Domain Controller. Sharing Group Policy objects, other policies, and scripts among all domain controllers in the domain can be made easier by this.

* 1. What is Loopback Processing, and when is it used?

>> With the use of Loopback Processing feature in Windows domain controller group policy, administrators can manage the settings for Group Policy that are applied to users when they log in to a particular user computer. Instead of the user account itself, it primarily depends on where the user account is located.

* 1. What is the difference between an Active Directory folder and an Organizational Unit?

>> Active directory folder is similar to a database that holds critical information about an organization including the details about the users, computers, and their defined scope.

It is the centralized controls for the user management and makes the life of the administrator easier. An OU is an active directory object or component which helps to organize all the components of the active director in the organization.

These OUs help in deploying the group policy settings to the set of users in the organization depending on their roles and requirements. Ou’s typically help in bifurcating the policies among the departments, for example in an organization.

* 1. What is slow link processing, and when is it used?

>> It is a method in which the windows client machine determines the throughput between the machine and the nearest domain controller before applying the GPO settings to check if the link between them is ‘slow’. If the throughput is lesser between the client machine and the DC then certain policy settings of GPO are not applied to make sure that the startup process doesn’t take a lot of time and slow down the user experience.

* 1. What is the difference between synchronous and asynchronous processing?

>> In synchronous processing the tasks are performed sequentially, and the tasks are dependent on the completion of the previous one whereas in asynchronous processing the tasks are performed independently without waiting for the previous ones to be completed. In the case of the group policy processing if used inefficiently there might be serious performance ramifications at the user end. The use of any of the above processing techniques depends on the requirement.

In **synchronous processing**, the users cannot see the desktop until the group processing completes, it significantly increases time required by the user to boot up the system and it gets it ready for use.

The **asynchronous processing** is also called the fast logon optimization where the windows system doesn’t wait for the completion of the group policy processing reducing the wait time for the user.

This assignment must be written in your own words. Any plagiarised content will result in a grade of 0 for the assignment. Include any sources that you use for your report.

***References***

(N.d.). Retrieved from <https://www.ultimatewindowssecurity.com/wiki/page.aspx?spid=KerberosPolicy>

Home. (n.d.). Retrieved from <https://itfreetraining.com/lesson/group-policy-loopback-processing/#:~:text=Loopback%20processing%20allows%20the%20administrator,user%20settings%20to%20be%20applied>.

Simplilearn. (2023). Retrieved from <https://www.simplilearn.com/what-is-kerberos-article#:~:text=Key%20Distribution%20Center%20(KDC)%3A,called%20the%20Key%20Distribution%20Center>

Simplilearn. (2023). Retrieved from <https://www.simplilearn.com/what-is-kerberos-article#:~:text=Key%20Distribution%20Center%20(KDC)%3A,called%20the%20Key%20Distribution%20Center>

(N.d.-a). Retrieved from <https://www.fortinet.com/resources/cyberglossary/kerberos-authentication#:~:text=Kerberos%20uses%20symmetric%20key%20cryptography,identification%20of%20all%20verified%20users>

(2023). Retrieved from <https://intellipaat.com/blog/what-is-kerberos/?US#no5>