**Servers Lab 3**

**Arnav Gupta**

**U1450149**

Comment: All uNID are mentioned inside a red box or red underline

Screenshot 1:

A screenshot of a computer

Description automatically generated

Screenshot 2:A screenshot of a computer

Description automatically generated

Screenshot 3:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Screenshot 4:

A screenshot of a computer

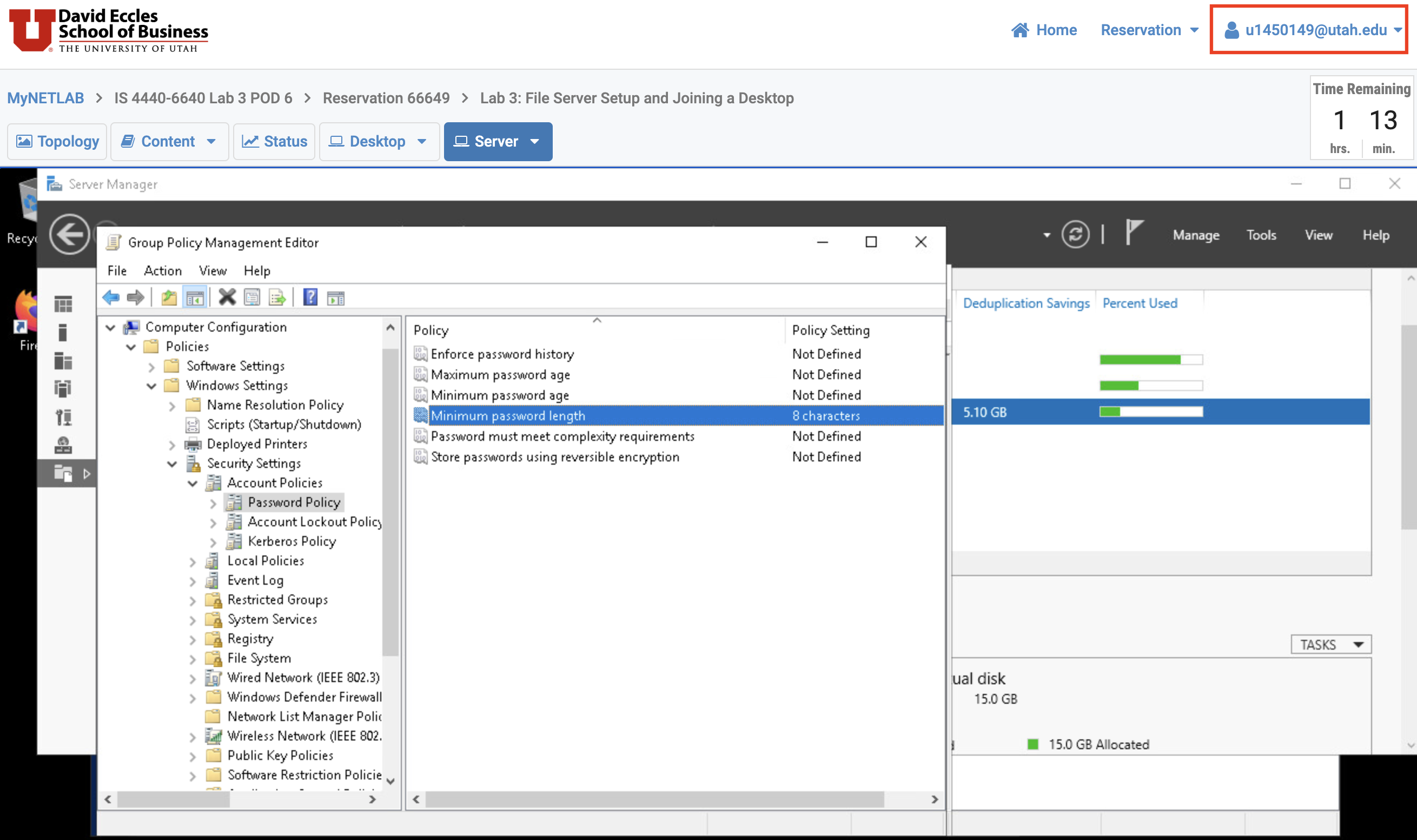
Description automatically generated

Screenshot 5:

A screenshot of a computer

Description automatically generated

Screenshot 6:



A computer screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Screenshot 7:

A screenshot of a computer

Description automatically generated

Screenshot 8:

A screenshot of a computer

Description automatically generated

**Additional Questions**

**Question 1**

The default setting of "Inherited Permissions" must be removed in order to restrict access to the "B:\Data\Finance" folder and configure NTFS rights. Permissions from parent folders are automatically applied to the child folder when they are inherited. By deleting inherited rights and granting the "Finance" folder explicit permissions to limit access, you would be able to break this inheritance.

**Question 2**

When mapping a shared folder to a specific local drive automatically, Group Policy Objects (GPOs) provide a number of benefits over manual techniques, especially in an enterprise setting. For this task, you may choose to use GPOs for the following two reasons, for example:

1. **Security and Access Control:** GPO-based drive mapping allows for enhanced security and access control. With GPOs, you can:

* Implement fine-grained access controls: You can define which users or groups have access to specific drive mappings, helping to restrict access to sensitive data.
* Enforce security policies: GPOs can be used to ensure that drive mappings comply with security policies, such as requiring secure connections (e.g., HTTPS or VPN) to access certain shared resources.

1. **Centralised Management and Consistency:** GPOs allow you to centrally manage your domain's drive mappings for multiple users or computers. Instead of configuring drive mappings on each computer individually, you can define them in one place and apply them universally. This ensures consistency and eliminates the risk of human error in configuring drive mappings manually on each computer.

**Question 3**

In Windows Server domains, the minimum password length by default is seven characters. Therefore, the default policy for the domain would be a minimum password length of 7 characters for all user accounts inside the domain if we had not specifically specified the "SLC Policy" to have a minimum password length of 8 characters.

**Question 4**

* Share tab on the “B:\Data\Finance” folder (“Advanced Security Settings for Data” window) and add it team’s AD group to have read-only access to the folder for audit.

• Effective Permissions Tab on the “B:\Data\Finance” folder (“Advanced Security

Settings for Finance” window) to review and verify the activity.

**Question 5**

Files and folders that users do not have authority to access are hidden in a shared location using Access Based Enumeration (ABE). Enhancing security, streamlining the folder hierarchy, and guaranteeing that users view only authorized content facilitates user navigation and thwarts unauthorized access.

**Question 6**

Improved Network Efficiency:

Decreased network congestion: You can maximize network efficiency by sending only unique data, particularly in scenarios when bandwidth is scarce, such distant offices or slow connections.

Faster data replication: Decumping reduces the amount of data transferred over the network, which increases the effectiveness and economy of replication for businesses who need to duplicate data across several sites.

Enhanced Data Integrity and Recovery:

Data consistency: By ensuring that several copies of the same data are consistent, deduplication lowers the possibility of data inconsistencies.

Faster recovery: Because only unique data needs to be restored, deduplication can speed up recovery times in the event of data loss or corruption, saving time and resources.

**Question 7**

* Data integrity is loss in case of relations in data, as the reference to data is combined to a single

reference.

* Using deduplication adds complexity and overhead to the system which leads to reduction in system

performance.