CCT College Dublin

Assessment Cover Page

Module Title:	Computing Architectures
Assessment Title:	Virtual Windows Active Directory / Network Server Virtualization
Lecturer Name:	Michael Weiss
Student Full Name:	Publio Lima de Mello Filho
Student Number:	2024028
Assessment Due Date:	20/05/2024
Date of Submission:	19/05/2024

Declaration

By submitting this assessment, I confirm that I have read the CCT policy on Academic Misconduct and understand the implications of submitting work that is not my own or does not appropriately reference material taken from a third party or other source. I declare it to be my own work and that all material from third parties has been appropriately referenced. I further confirm that this work has not previously been submitted for assessment by myself or someone else in CCT College Dublin or any other higher education institution.

Summary

This assessment offers a thorough rundown of the setup and configuration of a fully functional Domain Controller for DigiTech, a busy product services company. Including user accounts, Organizational Units (OUs), group rules, shared files, and other critical network resources, the Domain Controller is a key component in the management of the company's network infrastructure. We set up Accounting and Sales department OUs, create and arrange user accounts inside these OUs, and set up global security groups to simplify access control through a comprehensive set of actions. In addition, each department's shared files must be created, and certain permissions must be applied to provide safe and suitable access depending on group membership. Domain-wide password management and account lockout rules, which require frequent password changes and enforce lockouts following a certain number of unsuccessful login attempts, are put in place to improve security. In addition, a thorough explanation of how to set up a DHCP server is provided, along with instructions on how to configure IP address reservations, exclusions, and scopes for effective network management. Additionally, RAID setups are set up on the Web server to offer fault tolerance and protect important data from unintentional erasure. To further customize and safeguard the user experience, further customizations are put in place, such as setting separate departments' desktop wallpapers and limiting access to the Control Panel. The paper concludes by outlining the reasoning behind designating distinct logon times for various departments and stressing the significance of restricting network access to business hours in order to improve security. In addition to detailing the technical procedures followed, this paper highlights the advantages of each configuration, guaranteeing that DigiTech's network is stable, safe, and well-managed to meet its operational requirements.

Setting up the resources and network users:

Two Organizational Units (OUs) called Accounting-Dublin and Sales-Dublin will be built utilizing Active Directory Users and Computers (ADUC) in order to effectively organize DigiTech's network architecture. The user accounts and network groups for each department will be stored in these OUs. The Accounting-Dublin OU will host user accounts for accounting personnel, and access and permission management will be handled by the global security group named Accounting. To provide efficient and safe management of departmental resources and permissions, user accounts for sales personnel will also be created within the Sales-Dublin OU, along with a global security group called Sales.

Accounting will be the name of the Global Security group that will be established inside the Accounting-Dublin Organizational Unit (OU). The names that have been provided will then be used to create five user accounts: Barb Dwyer (dwyer), Adam Baum (abaum), Patrick Joseph Jones (pjjones), and Al Bino (abino). The password "pass1234!" will be automatically changed at first login for each account. A Global Security group called Sales will also be established in the Sales-Dublin OU, and five user accounts—Claire Morris (cmorris), Claire Galway (cgalway), Annabelle Lecter (alecter), Anna Conda (drdoran), and Justin Case (jcase)—will be created with the same initial password policy. See table below:

Patrick Joseph Jones (Accounting) Username: pjjones	Claire Morris (Sales) Username: cmorris
Patrick Leroy Jones (Accounting) Username: pljones	Claire Galway (Sales) Username: cgalway
Adam Baum (Accounting) Username: abaum	Annabelle Lecter (Sales) Username: alecter
Barb Dwyer (Accounting) Username: dwyer	Anna Conda (Sales) Username: drdoran
Al Bino (Accounting) Username: abino	Justin Case (Sales) Username: jcase

The following screenshots will show the groups with the users created in their respective groups:

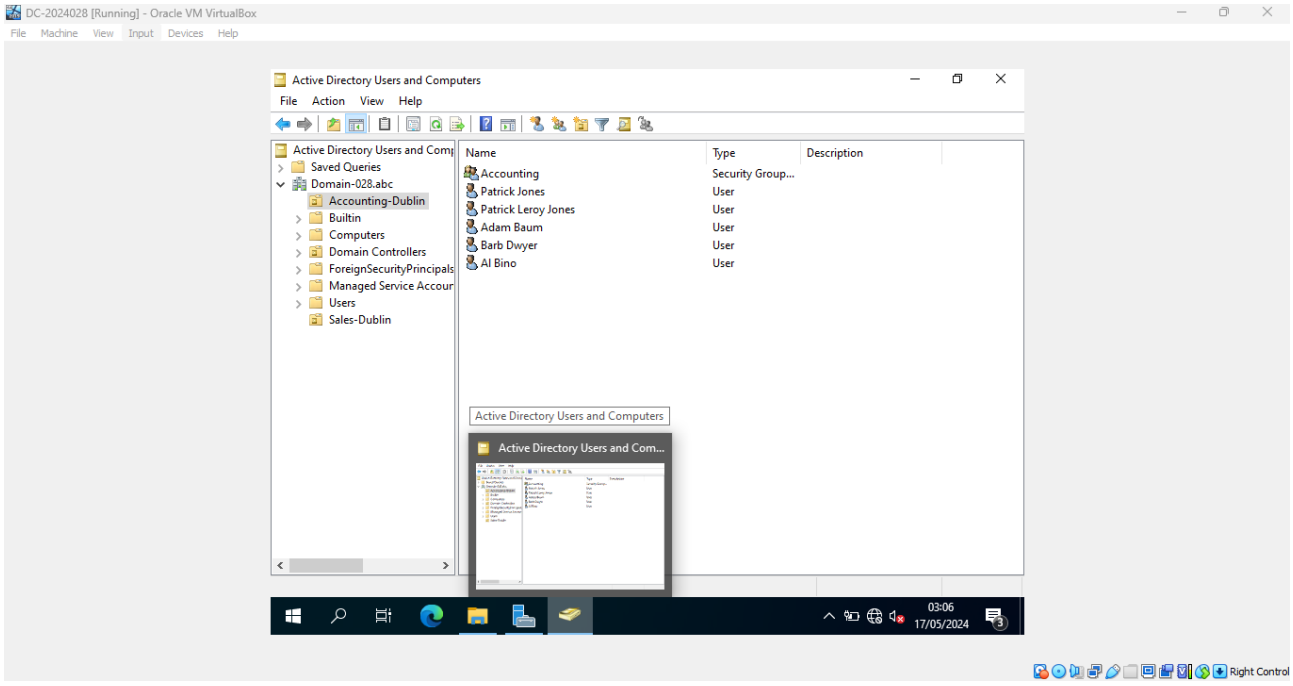

Image 1: Accounting- group.

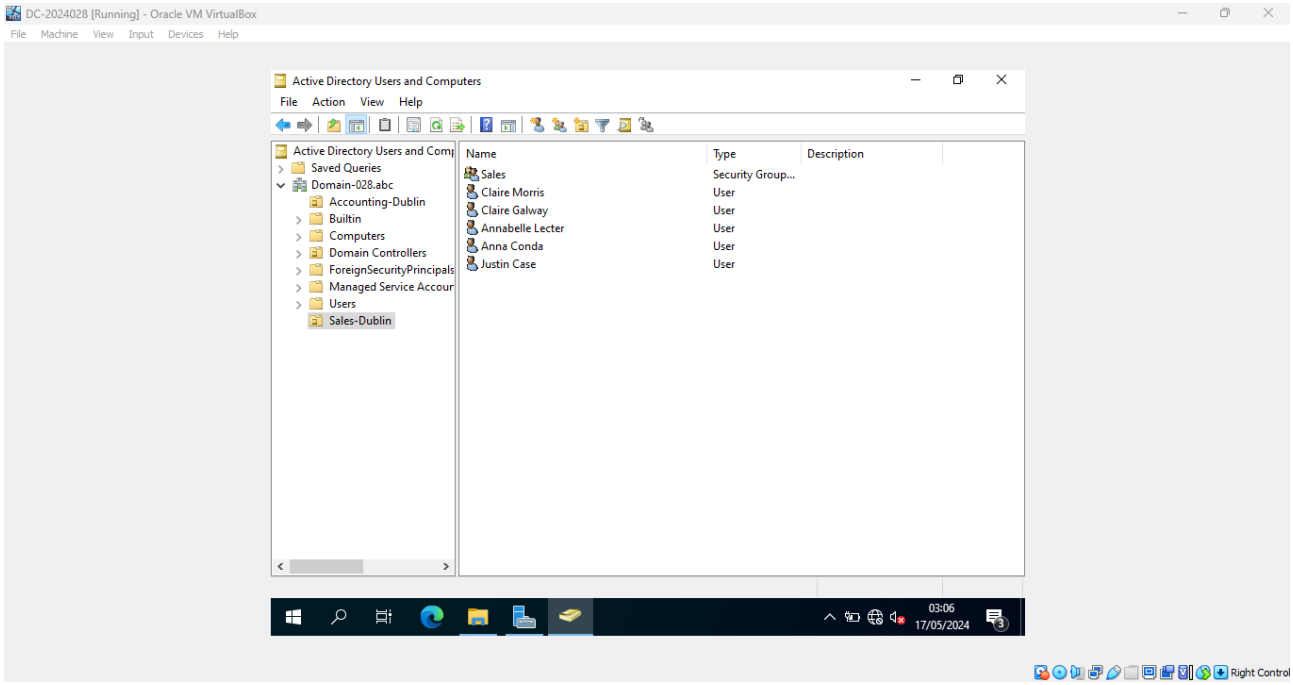

Image 2: Sales Group.

Applying both NTFS and Share permissions is necessary to guarantee that departmental folders have the proper access control. Permissions for the Sales-Documents folder should be set to Full Control, giving the sales group full control over and access to all files contained therein. In a same vein, the Accounting group ought to have complete access privileges by being granted Full Control permissions for the Accounting-Documents folder. In order to improve security while creating these sharing settings, it is imperative that the Everyone group be removed from the permissions list. By establishing permissions on both the Security and Share tabs, this two-tiered method guarantees accurate and strong access control, safeguarding the confidentiality and integrity of departmental data.

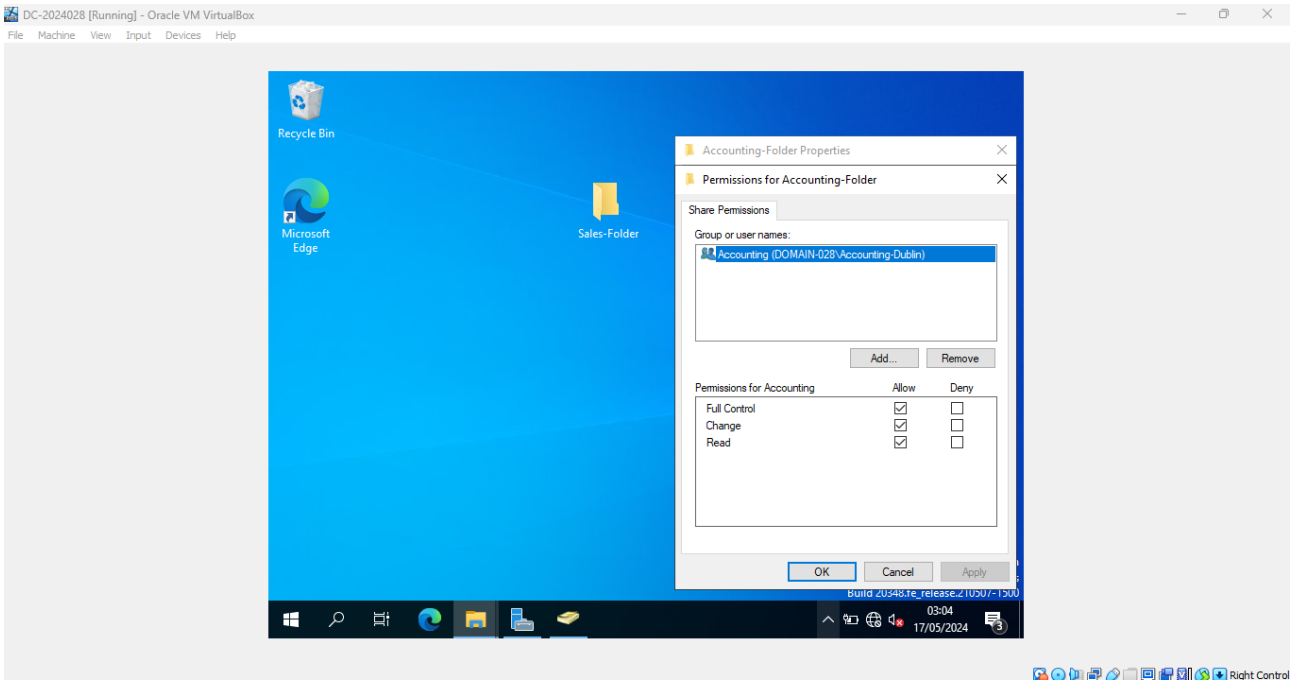

Image3: Accounting sharing.

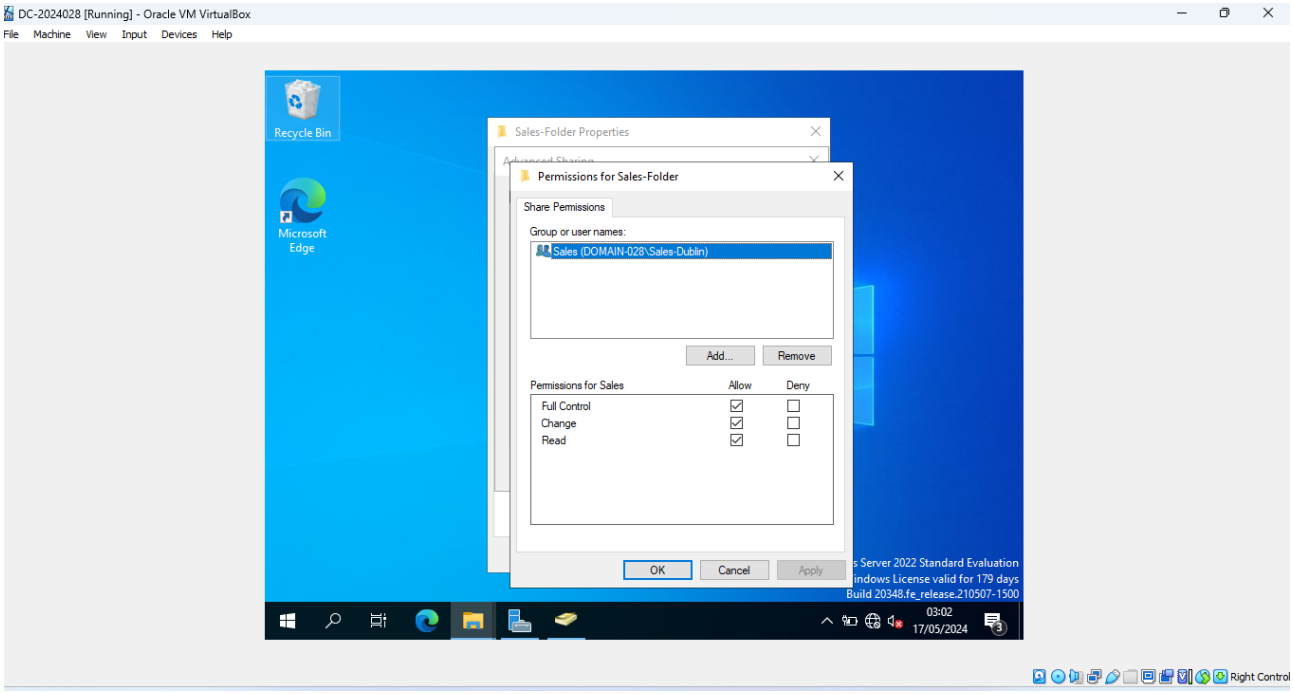

Image 4: Sales sharing.

To verify the permissions for both the Sales-Documents and Accounting-Documents folders, conduct a series of tests by logging into the Web computer using user accounts from either the Sales-Dublin or Accounting-Dublin Organizational Units. For instance, a user from Sales-Dublin should be able to access the Sales-Documents folder but should be restricted from accessing the Accounting-Documents folder. Conversely, a user from Accounting-Dublin should have access to the Accounting-Documents folder but not the Sales-Documents folder. During the initial log-in, if prompted to change the password, use "pass1234$" as the initial password, in line with the password policy previously established. These tests ensure that the implemented permissions are correctly configured and enforce the intended access controls.

Accessing Sales.
User: Justin Case
Username: jcase
Password: pass1234!
New password: pass1234$

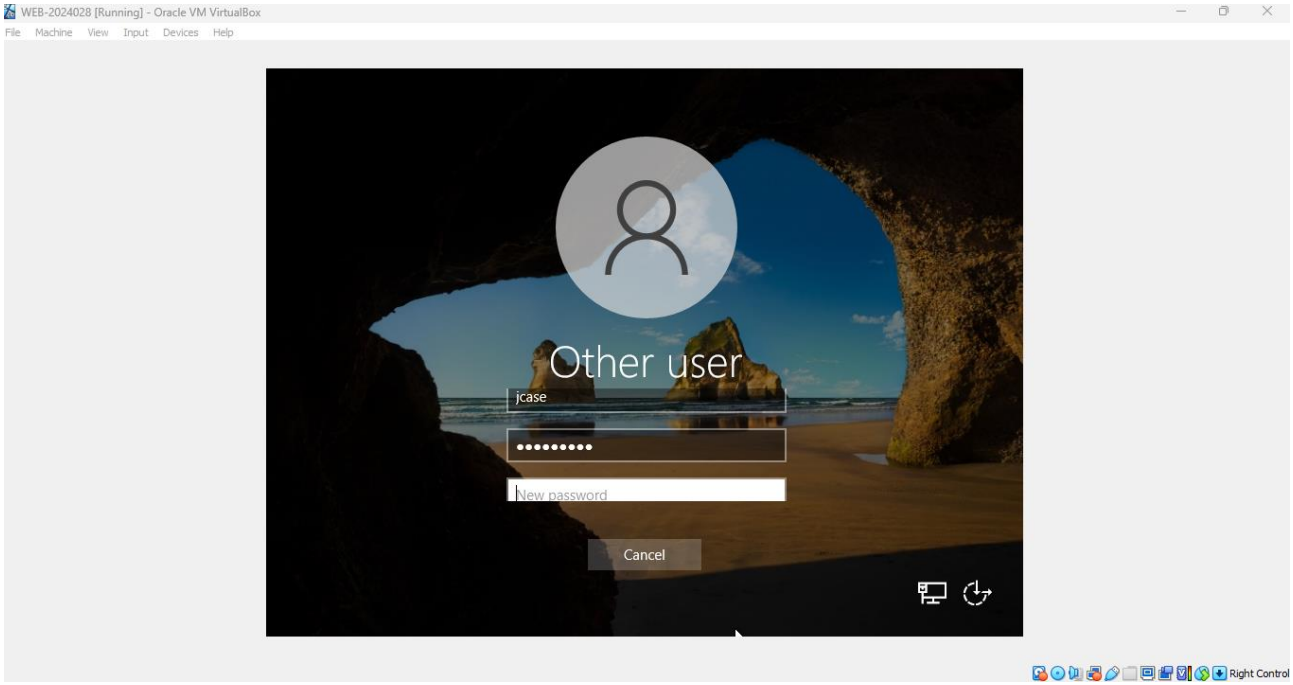

Image 5: Changing the password for jcase (Justin Case)

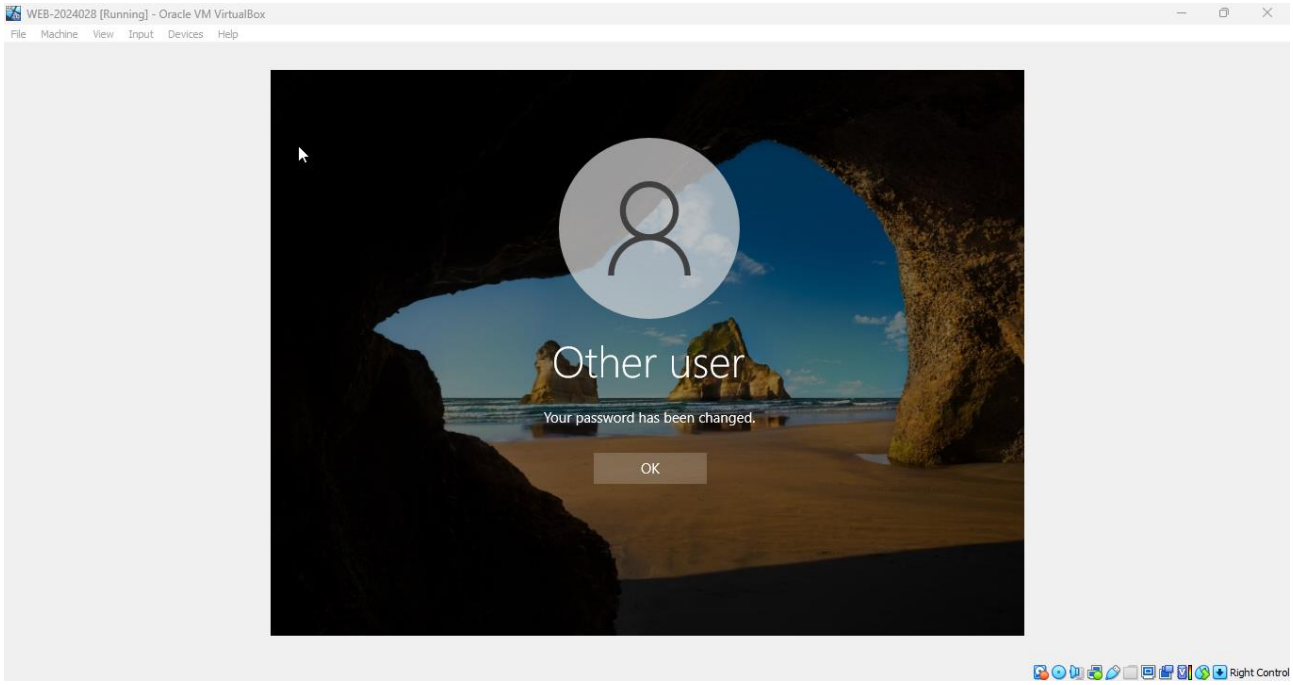

Image 6: Password successfully changed.

Verify the permissions for both resources using UNC format: \\Server-name\Shared-name Return to the Domain Controller and perform troubleshooting if the permissions are not working! Verifying the authorization of the resources: You need to be able to provide proof that the Account and Sales folder permissions are being honoured. For instance, you should be able to access the Sales_Documents folder if you log onto the Web server as a member of the Sales group, but Access Denied appears on the Accounting folder. As showed below:

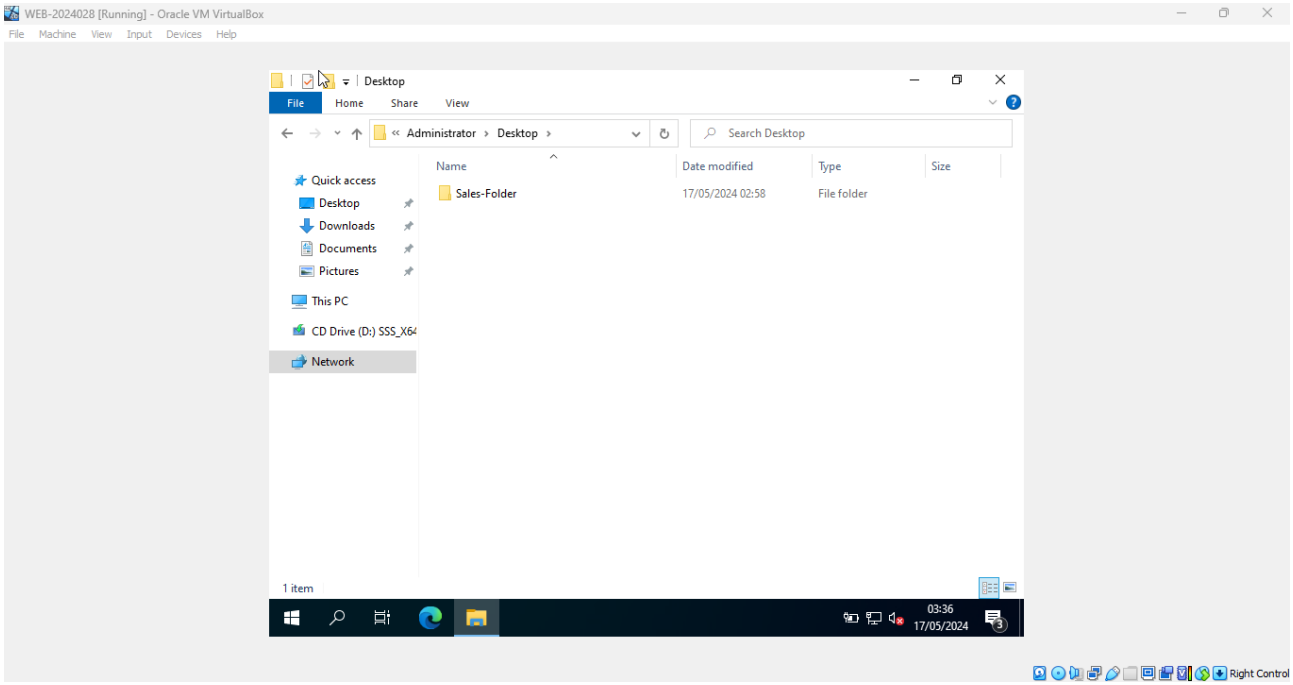

Image 7: Successfully connected to Sales folder

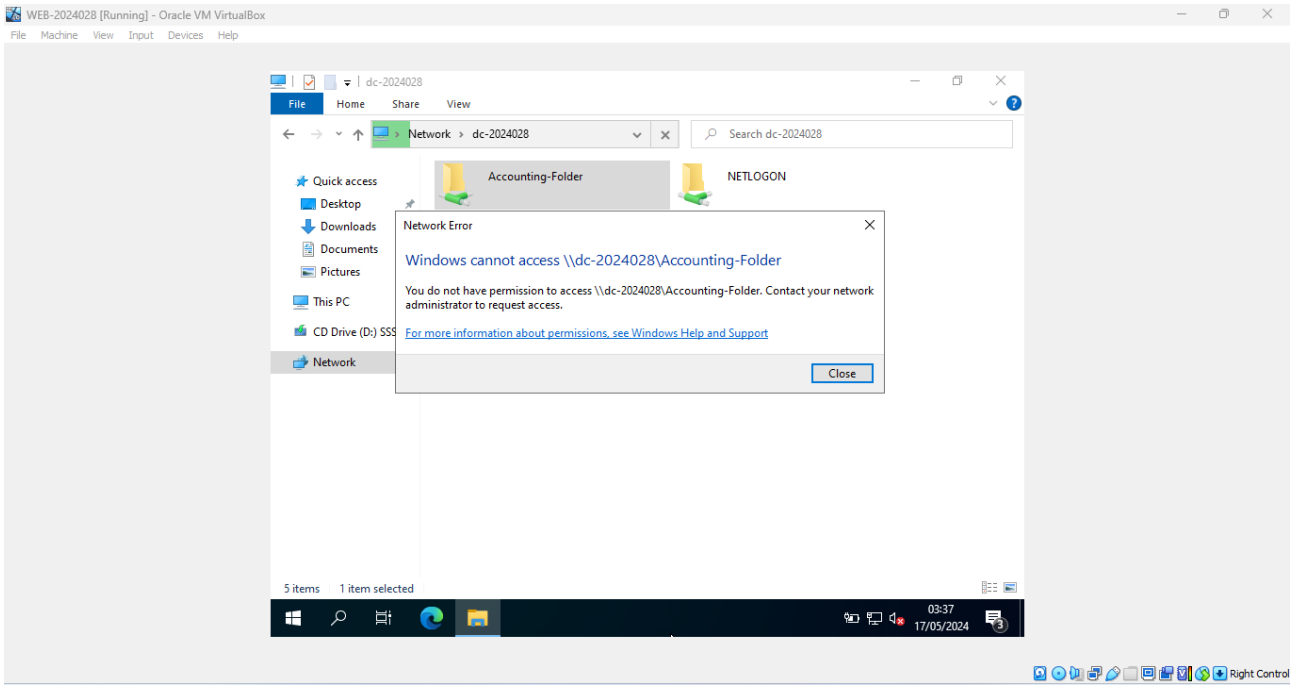

Image 8: Successfully denied for the accounting folder.

To improve security and stop unwanted access, a thorough password policy and account lockout policy have been put in place for the entire domain. In order to maintain password security over time, the password policy requires users to update their passwords every 30 days. Furthermore, a policy for account lockout has been implemented to safeguard against brute force assaults. This policy locks out user accounts following a certain number of unsuccessful attempts at logging in.

By working together, these steps improve the domain's security posture and lessen the chance that private data may be accessed by unauthorized parties.

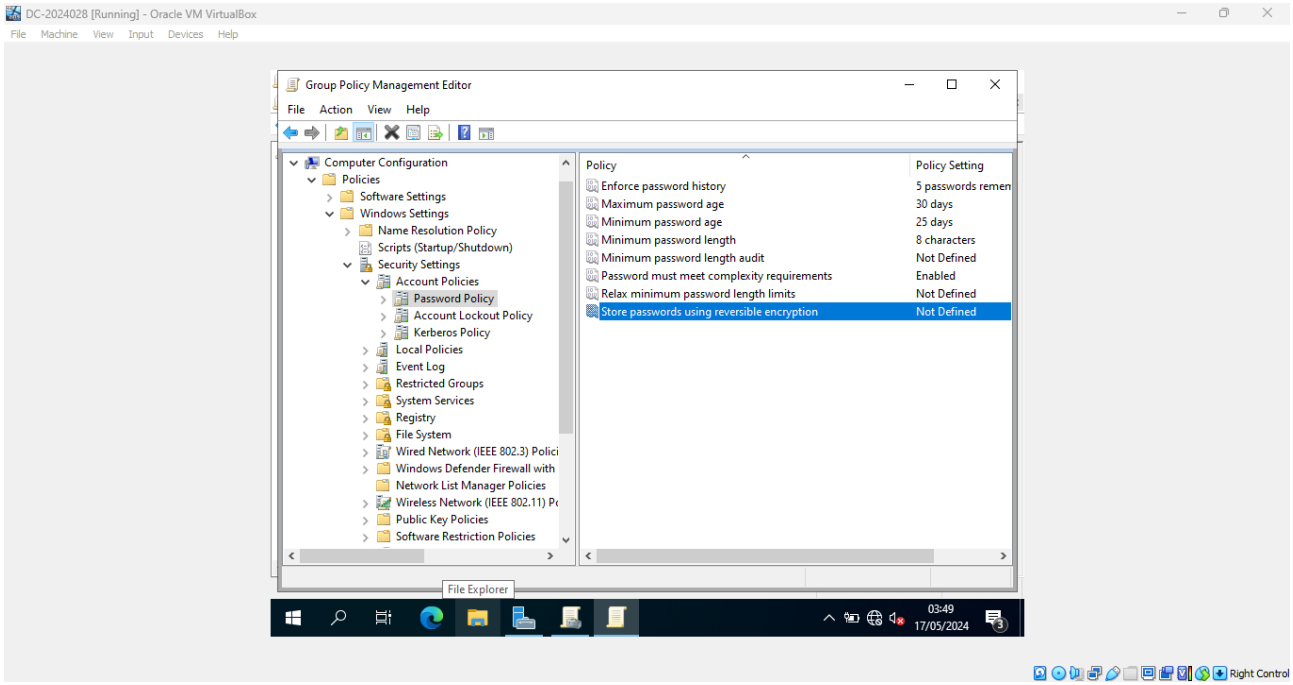

Image 9: Password policy applied

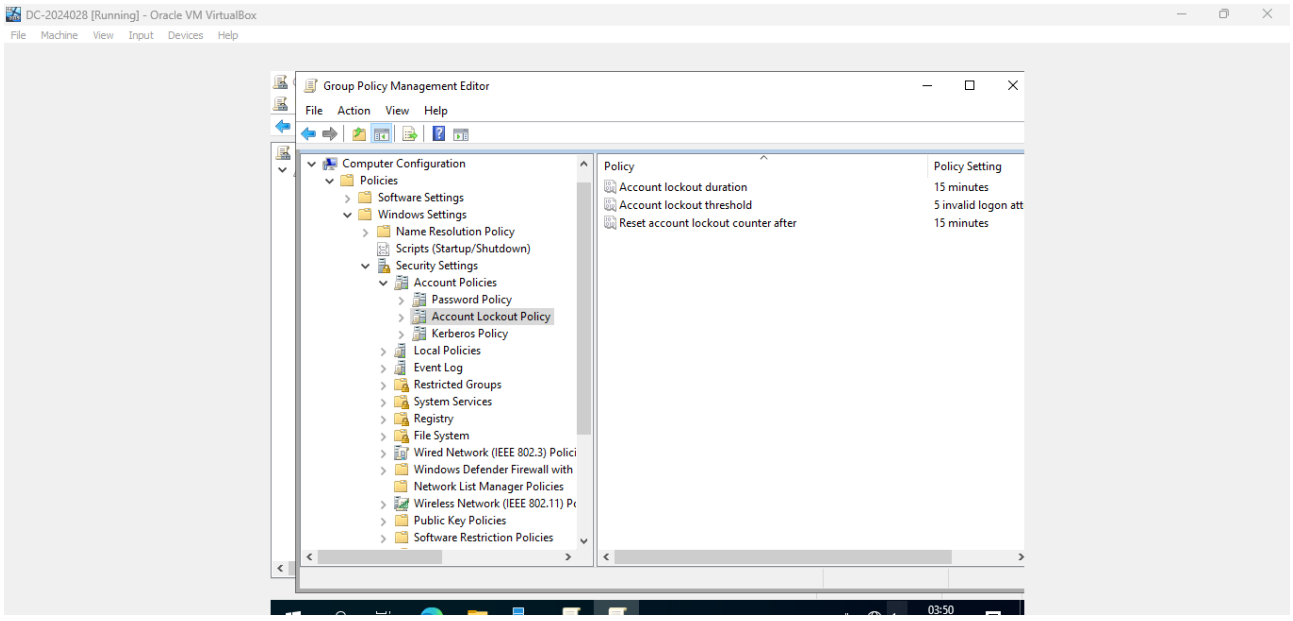

Image 10: Lockout policy applied.

Setting Up a DHCP Server for the Domain

The DigiTech Domain Controller server computer now has the DHCP server role added in order to enable dynamic IP address assignment for every client computer in the network. The DHCP server role was installed after choosing "Add Roles and Features" in the Server Manager console to complete this setup.

The DHCP console in Administrative Tools was used to configure the DHCP scope in compliance with the instructions provided. The IP address range from 172.16.0.1 to 172.16.0.254 was covered by the scope name "Domain-002," which had a default gateway of 172.16.0.1 and a subnet mask of /16. The lease period was set to 24 hours, and the DNS server IP was given as 172.16.0.100. To make sure that some IP addresses are not assigned dynamically, four DHCP address exclusions were also made.

Additionally, the Web computer's address was reserved through the DHCP console, which was accessed through Administrative Tools. Using IPCONFIG/ALL, the MAC address of the Web computer's network card was discovered, and a reservation with the name "Web 2024-028"—where "028" stands for my student number's final digits—was made. 172.16.0.50 is the IP address that was assigned to this reservation.

Lastly, rather than use a static IP address, the Web computer was set up to dynamically obtain its IP address from the reservation. By doing this, you may be confident that the Web computer will always connect to the network using the reserved IP address.

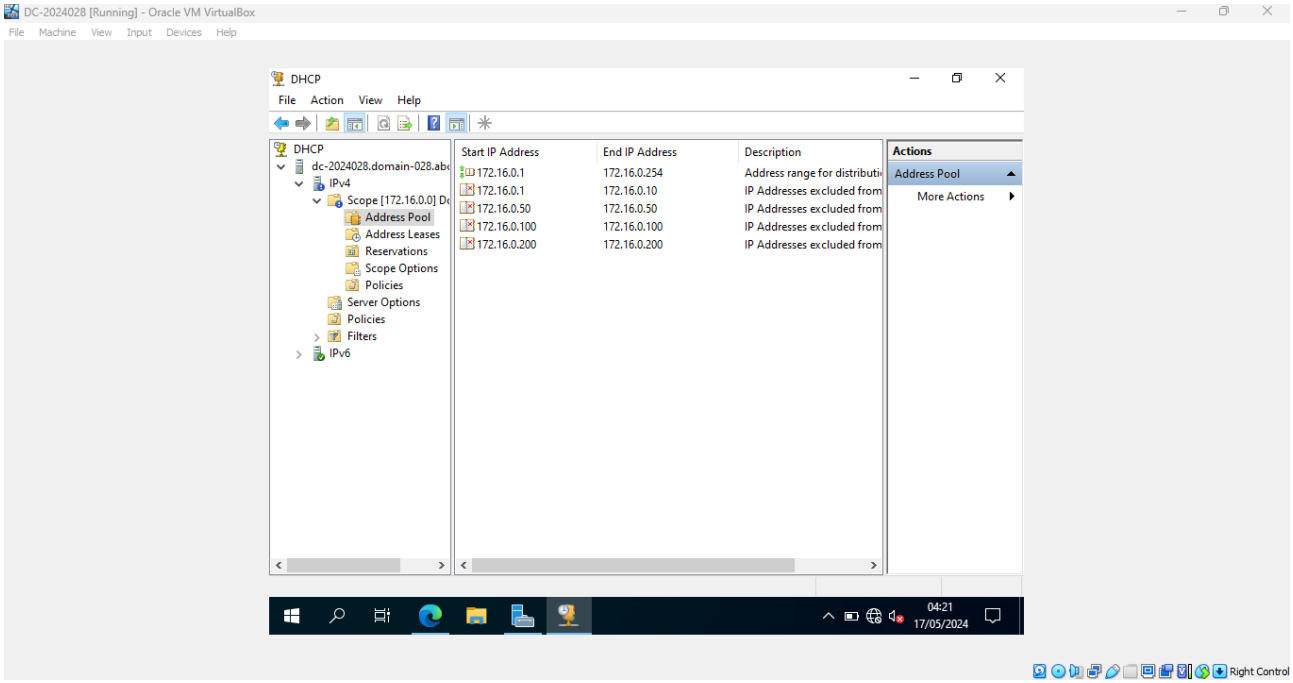

Image 11: Scope created.

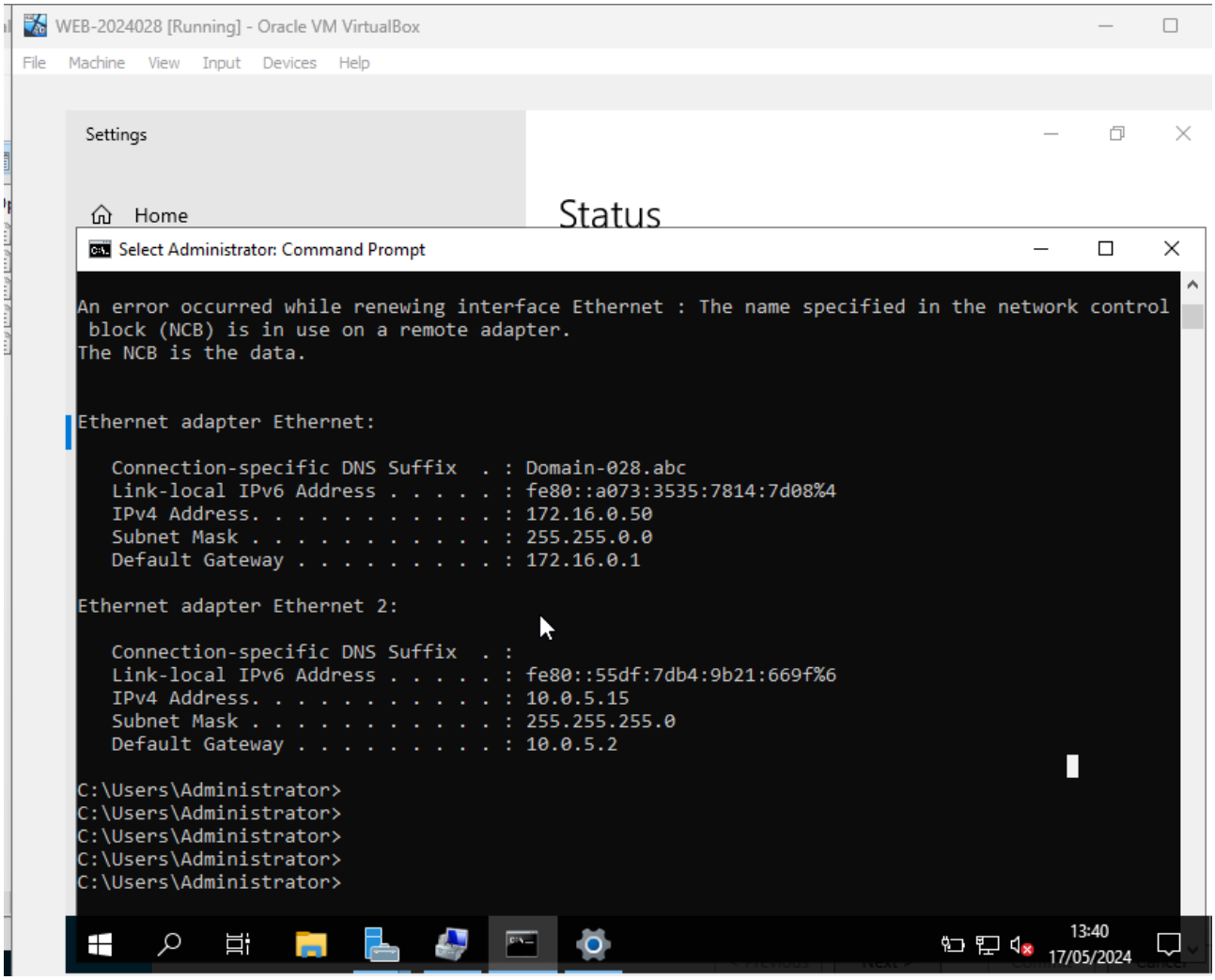

Image 12: IP config working.

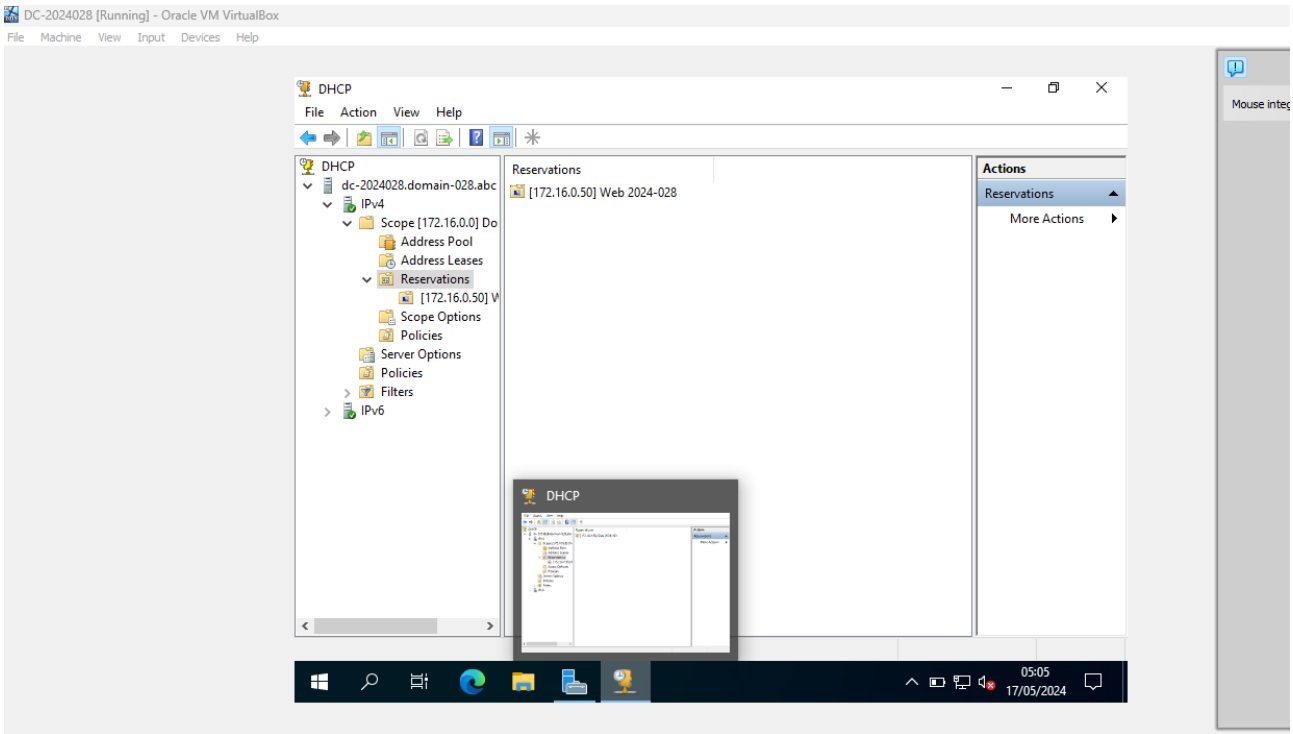

Image 13: Reservation completed.

Configuring RAID on the Web Server

Fault tolerance measures are being introduced by adding six more hard drives to the Web Server virtual machine (VM) in order to address the worry over possible data loss on the Web server. Drive D serves as the CD-ROM drive and Drive C serves as the server's primary volume at the moment. RAID configurations will be used to create two new volumes with fault tolerance.

First, a RAID 5 volume called Drive E: will be established using four of the extra disks. By spreading data among several drives with parity information, RAID 5 offers fault tolerance and enables continuous operation even in the event of a disk failure. This configuration increases overall reliability and guarantees data redundancy.

Second, two of the hard drives will be used to create Drive F:, a RAID 1 Mirrored volume. In order to provide redundancy and guarantee that data is preserved even in the event of a disk failure, RAID 1 Mirroring duplicates data across two disks. Because identical copies of the data are kept on both disks, this architecture provides a higher level of failure tolerance.

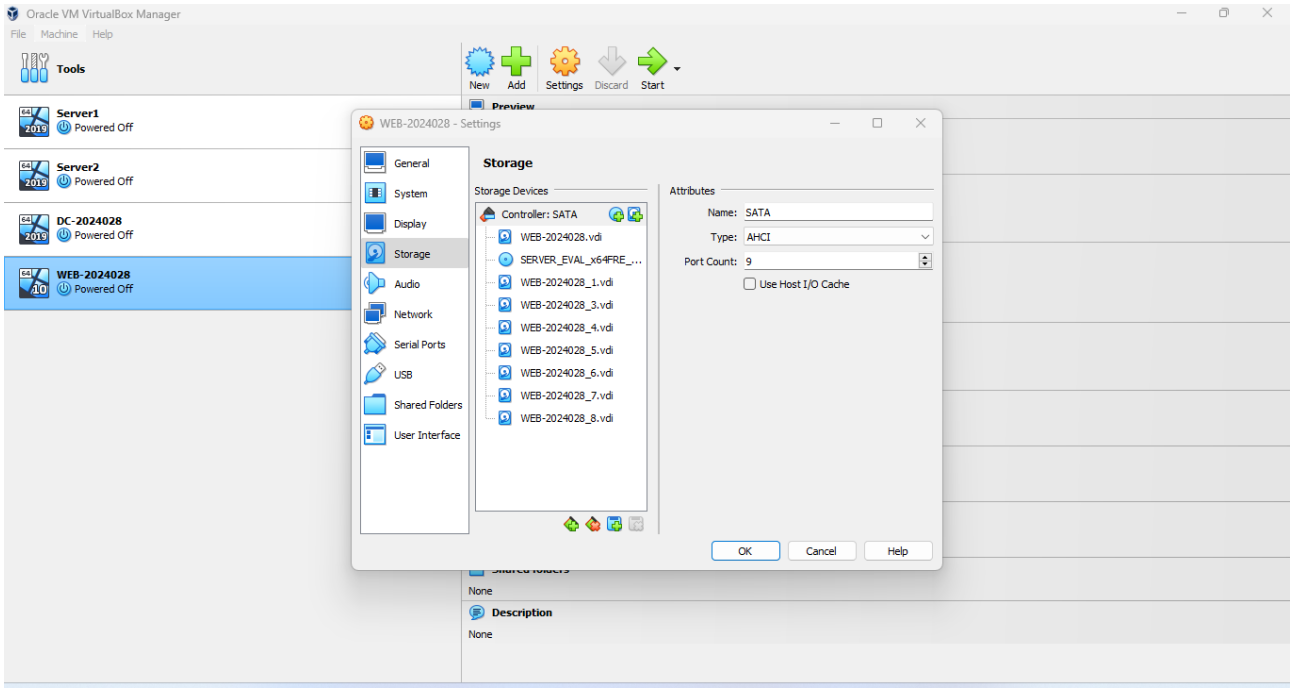

Image 14: Hard drivers created.

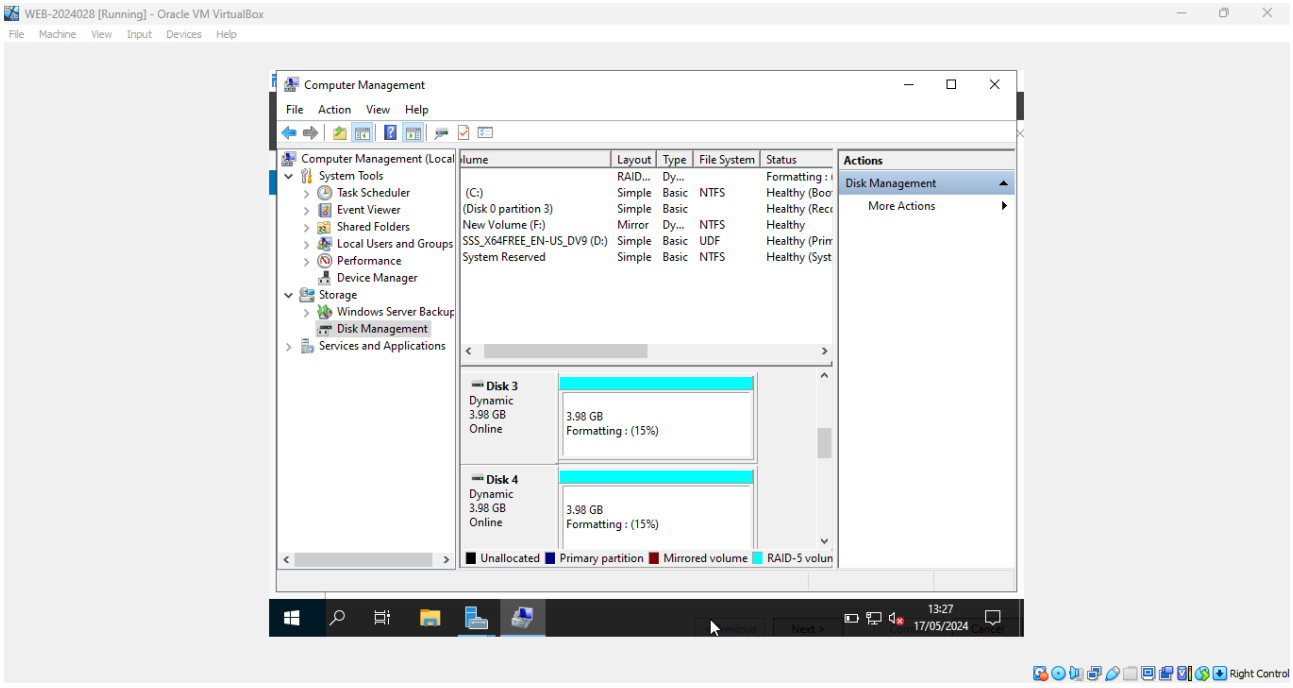

Image 15: Raid-5 created.

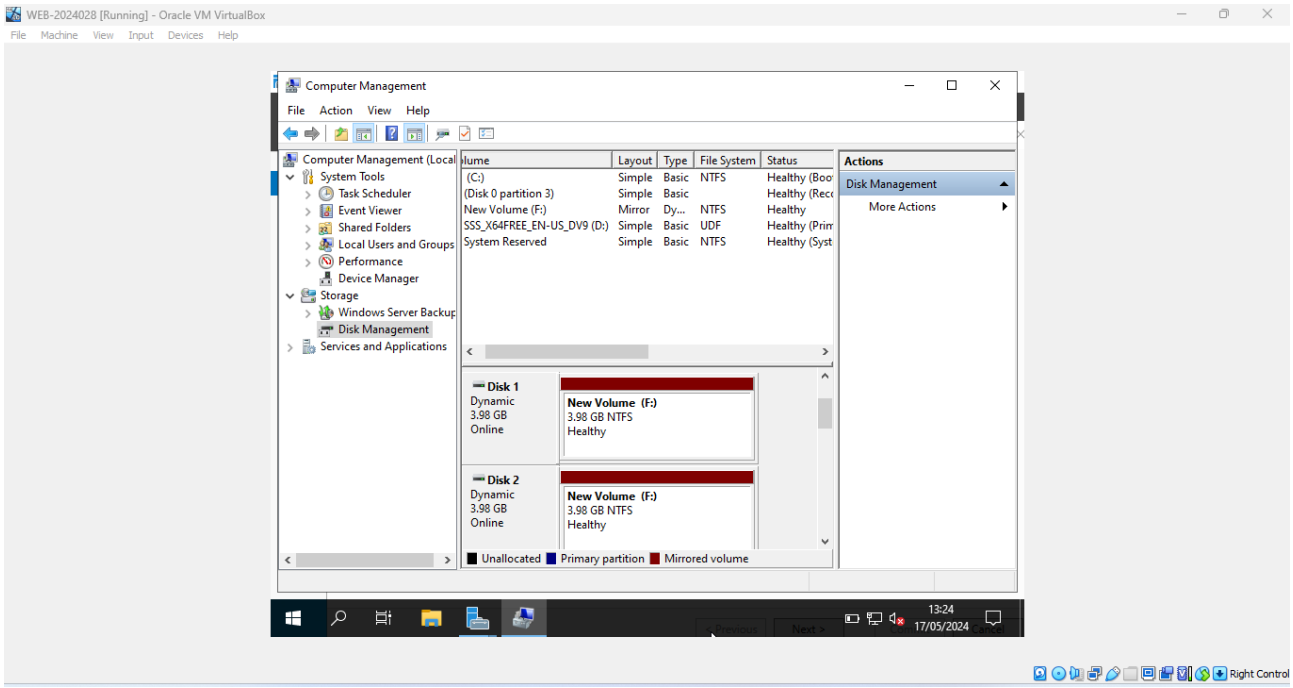

Image 16: Mirrored Raid 1 created.

The tasks above provide a foundation for a network infrastructure

Our plan is to utilize Group Policy Objects (GPOs) to set desktop backdrops based on department membership, so that every department at DigiTech has a unique wallpaper. We'll use the JPEG files from Moodle, which are accessible to the Sales and Accounting divisions, as wallpaper. Upon logging in, members of the Accounting department will view the Accounting-Department wallpaper, and members of the Sales department will see the Sales-Department wallpaper. By giving each

department, a visually unique desktop environment and encouraging a feeling of identity and organization within the business, this configuration will improve the user experience. Below are screenshots showing the implementation and it working.

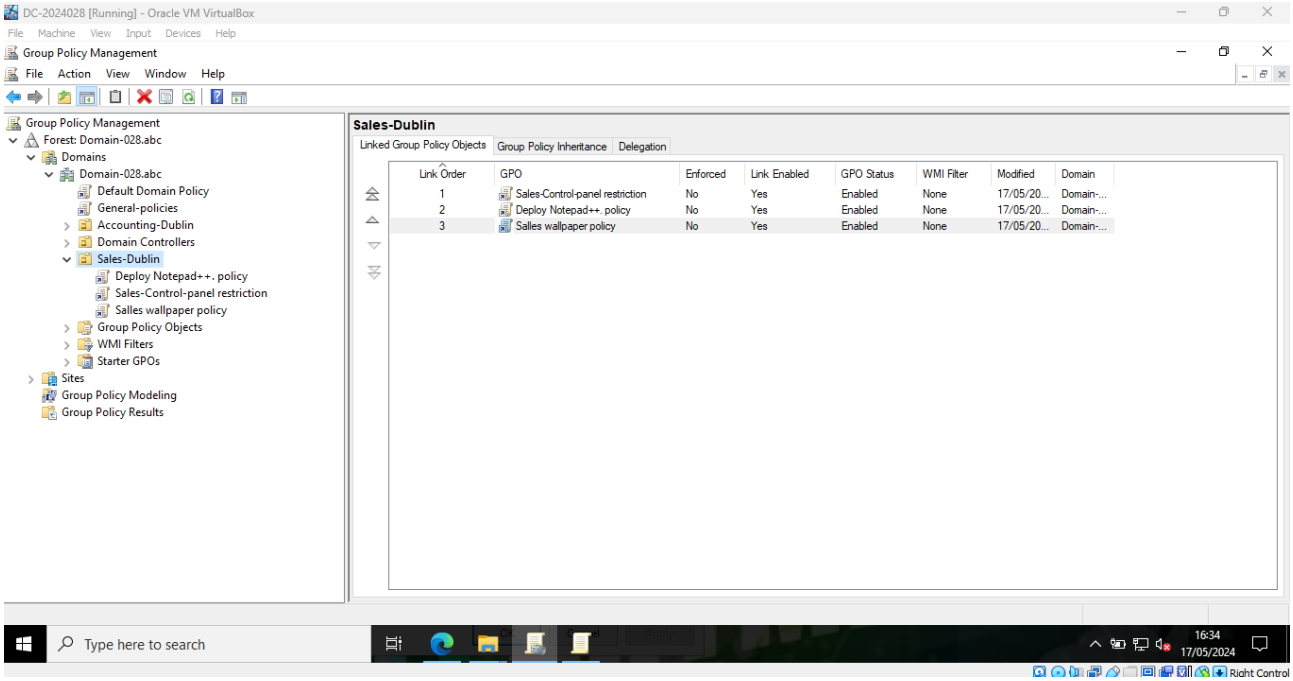

Image 17: Wallpaper policy created.

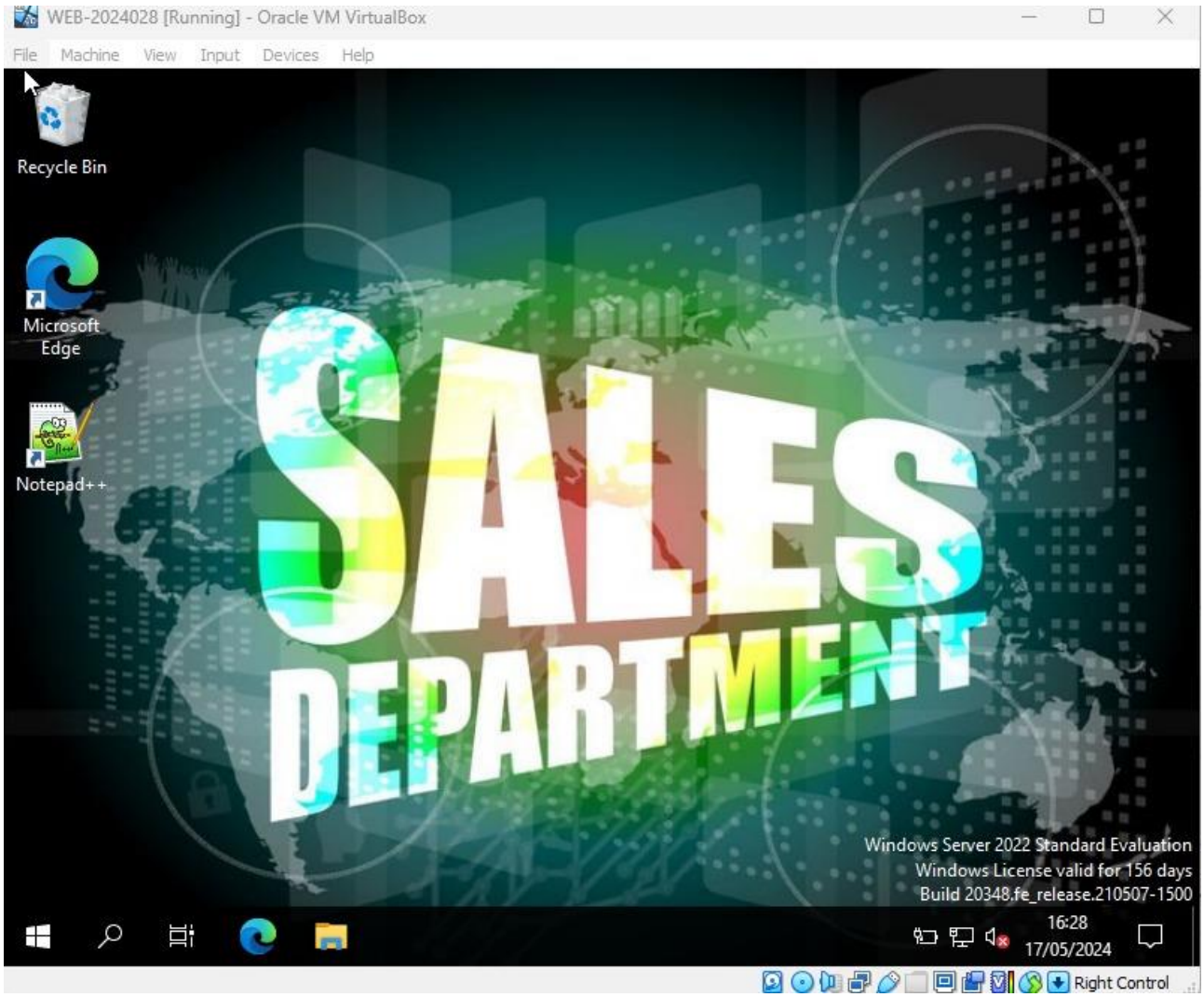

Image 18: Wallpaper working.

The Chief Information Officer (CIO) has ordered the termination of regular users' access to the Windows Control Panel due to unlawful changes made by users in the Accounting and Sales departments via the Control Panel. Group Policy settings can be used to accomplish this; in particular, a policy can be configured to hide the Control Panel icon from the desktop and Start menu. Users will be prevented from making unauthorized changes to their systems by enforcing this policy, which will prevent them from having direct access to the Control Panel. By taking this proactive step, security is improved and system configurations are kept intact and in accordance with company requirements.

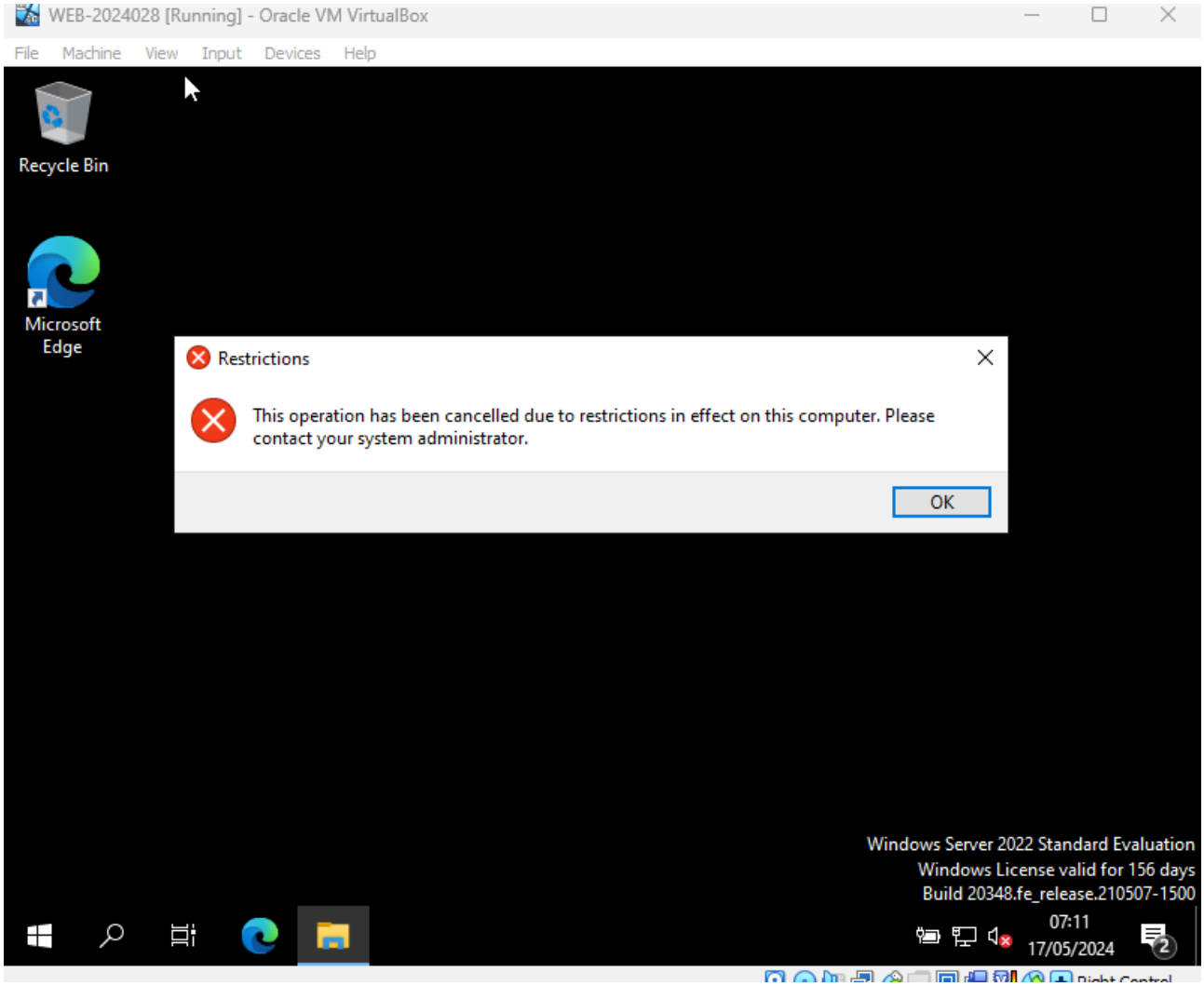

Image 19: Access denied for the control panel

The Sales group will be able to log in between 8:00 AM and 6:00 PM, whereas the Accounting group will only be able to do so between 9:00 AM and 5:00 PM in order to improve security and guarantee appropriate access control. These measures aim to reduce the risk of unauthorized access outside of working hours and ensure activities are monitored and controlled during designated times. Specifically, they are designed to limit access to sensitive financial data for the Accounting group during business hours and to accommodate the early and late working hours often required by sales operations.

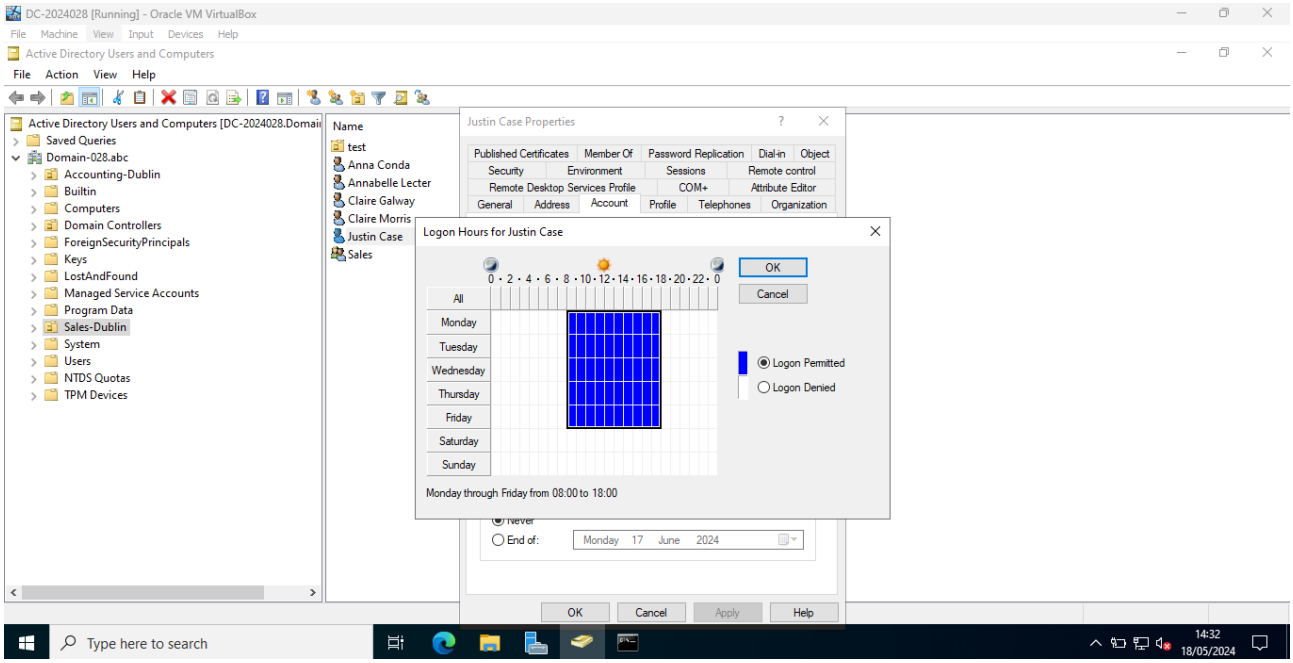

Image 20: Setting logon hours.

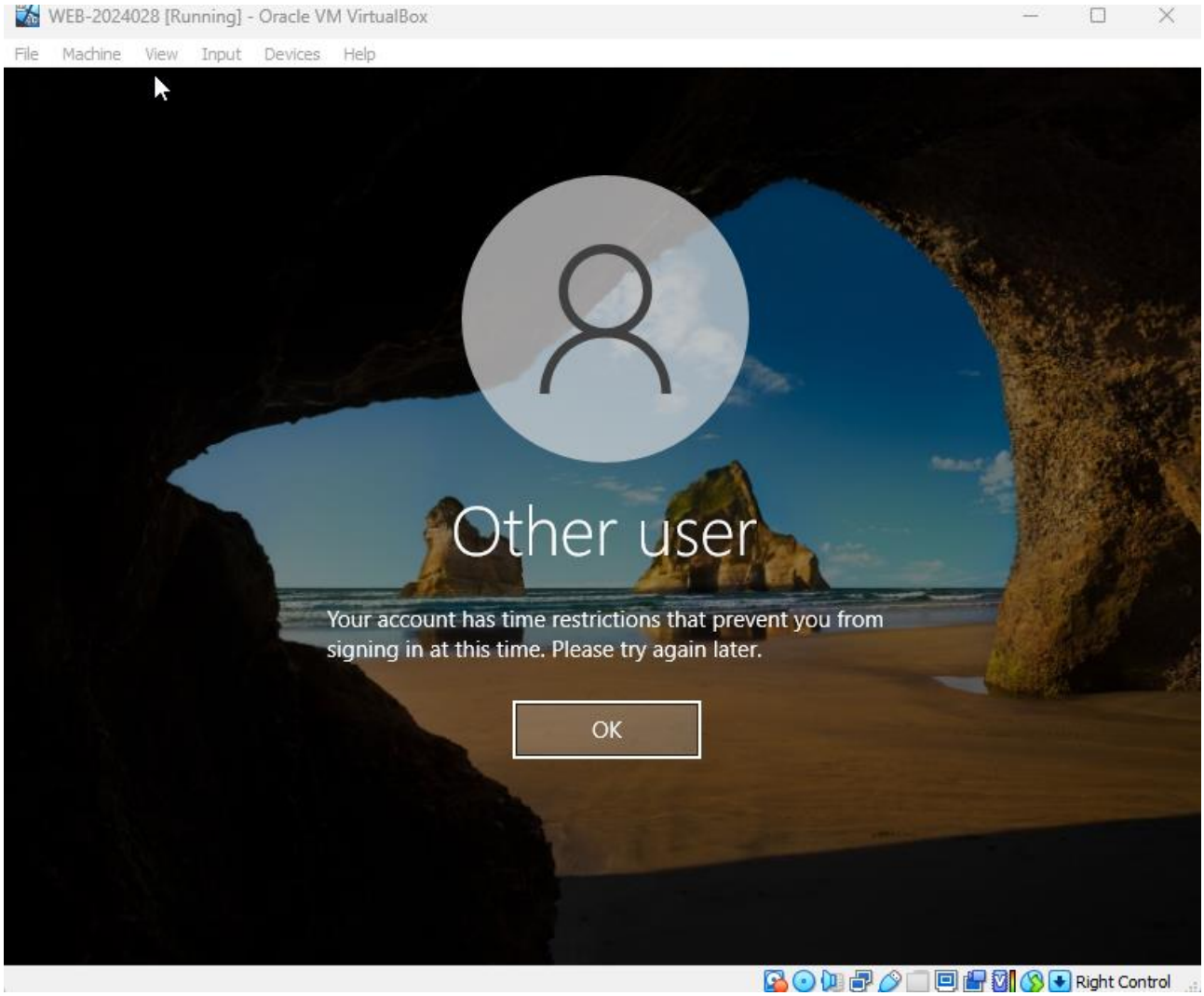

Image 21: Logon denied.

Restricting logon hours ensures that user access is restricted to their official working hours, which improves security. This lowers the possibility of unwanted access during off-peak hours when security may be laxer. Limiting logon hours for the Accounting department to 9 AM to 5 PM is in line with regular office hours and guarantees that users can only access critical financial data during supervised periods. The Sales department's longer hours are also accommodated by granting them access from 8 AM to 6 PM, which reflects their requirement to start early or stay late to finish sales efforts. These customized logon schedules aid in striking a balance between security and operating efficiency.

Several actions were done in order to enable the automated installation of Notepad++ for users in the sales department using Active Directory Group Policy. At first, the Notepad++ MSI package was downloaded from the specified site on the Moodle webpage. This MSI file was then copied to a shared network location that staff members in the sales department could access. Within the Group Policy Management Console (GPMC), a new Group Policy Object (GPO) was made and connected to the Sales department Organizational Unit. The Notepad++ MSI package was distributed within this GPO using the "Assigned" deployment method, which guarantees that Sales users will automatically install it when logging in. To speed up the installation process, configuration settings were changed when needed, and a group policy update was implemented. After doing these steps, Notepad++'s successful installation and operation were tested by logging into the Web Server using the Sales group's credentials. To offer visual proof of the deployment process and its results, screenshots of the Group Policy Management Console settings and the Web Server interface displaying Notepad++ were taken.

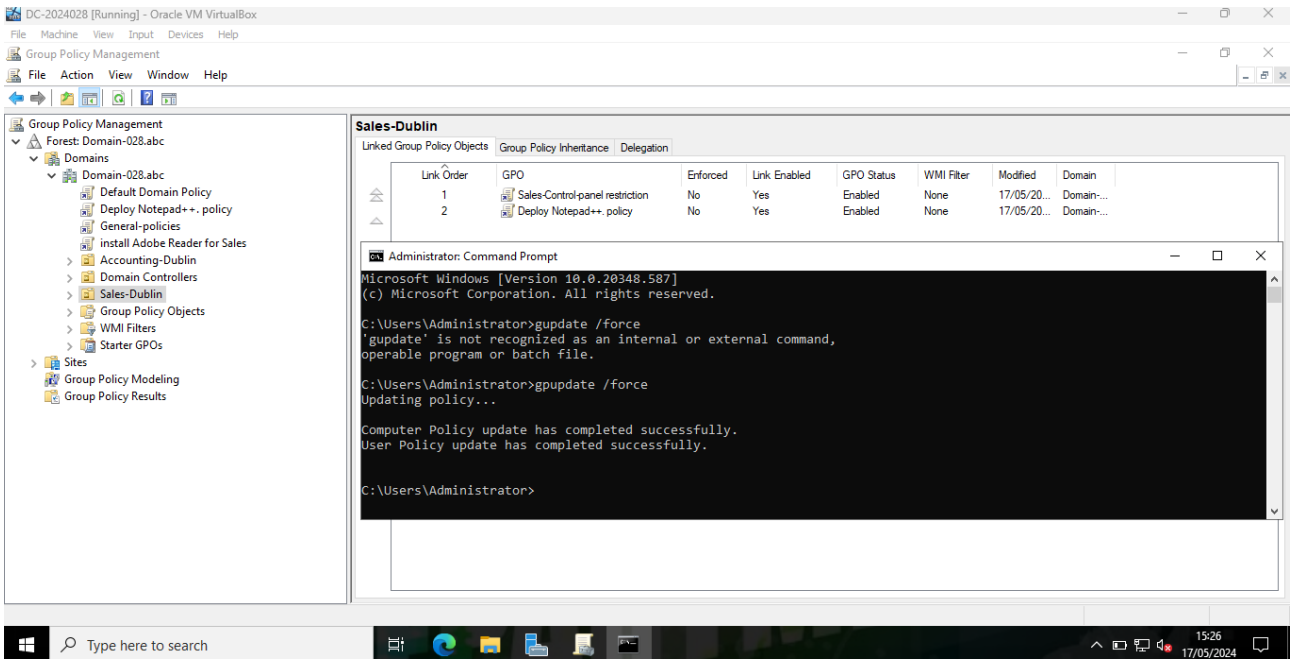

Image 19: Policy created for Notepad++.

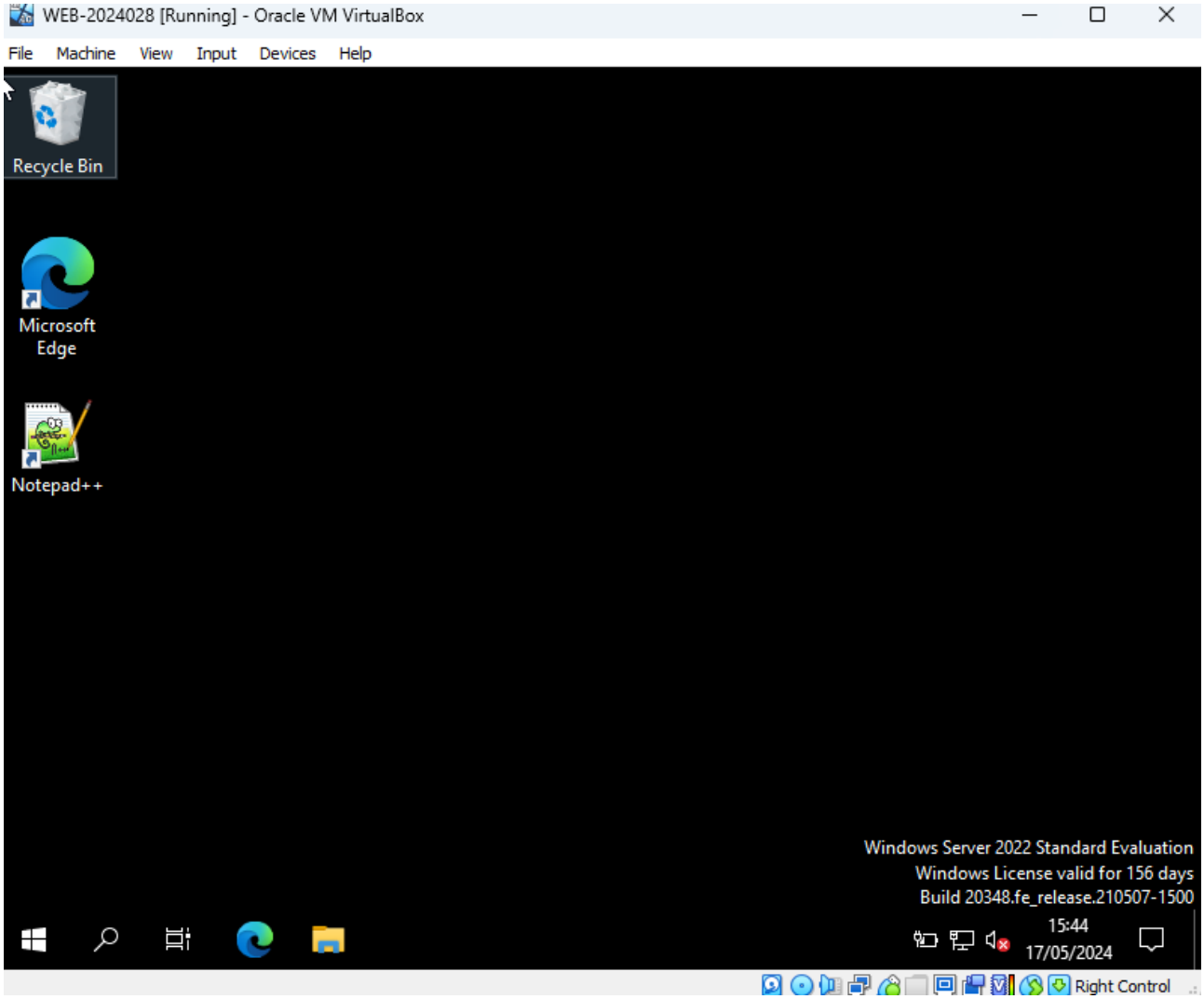

Image 20: Notepad++ successfully installed in a Sales user.

Similar steps were done as with Notepad++. Configuration settings were modified where necessary, and a group policy update was implemented, in an attempt to speed up the installation process. But even after doing all of this, the Adobe Acrobat Reader installation failed. By utilizing the Sales group's login credentials to access the Web Server and seeing that Adobe Acrobat Reader was not installed, the failure was verified. To record the deployment procedure and emphasize the problems encountered, screenshots of the Web Server interface and the Group Policy Management Console settings were captured.

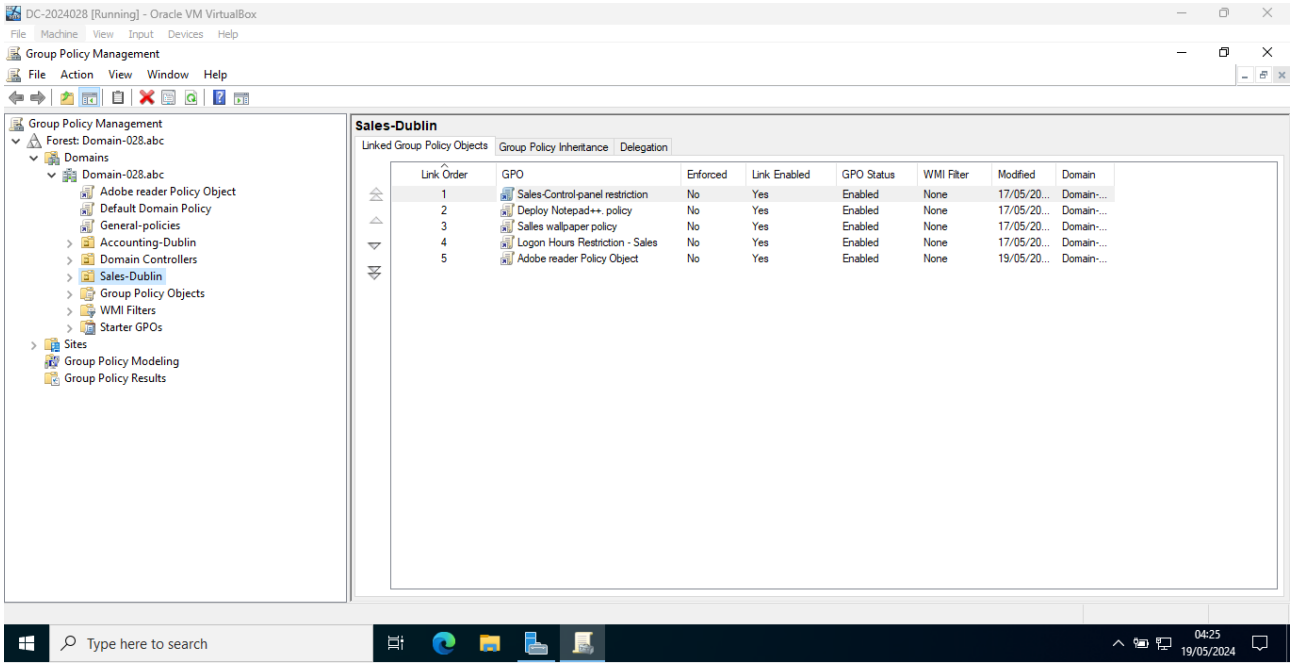

Image 21: Adobe policy created.

DigiTech asked to use an FTP server to make their "Employee Handbook" available on their website. I was tasked by the IT manager with installing this FTP server in the accounting department, which had previously been equipped with Adobe Reader. The intention was to make the DigiTech-Acceptable-Use-Policy document available to any user in the Accounting Department upon request by enabling the FTP server to distribute the PDF version of the document. I tried my hardest to follow all the instructions, including setting up the FTP server, but I was not able to finish this assignment. I tried my hardest, however I ran into problems that made the FTP server unable to operate as required.

References:

- [1] https://www.raspberrypi.org/about/

- [2] https://www.raspberrypi.org/documentation/

- [3] https://www.arduino.cc/en/about-us

- [4] https://www.arduino.cc/en/reference/homePage

- [5] Banzi, M., Shiloh, M., & Cuartielles, D. (2014). Getting Started with Arduino (3rd ed.). O'Reilly Media.

- [6] Monk, S. (2016). Programming Arduino: Getting Started with Sketches (2nd ed.). McGraw-Hill Education.

- [7] M. H. Cohen, "A Tribute to Seymour Cray," IEEE Spectrum, vol. 15, no. 2, pp. 67-75, 1978.

- [8] . M. Snyder, "The Contributions of Seymour R. Cray to Computer System Architecture," IEEE Annals of the History of Computing, vol. 22, no. 3, pp. 6-15, 2000.

- [9] D. A. Patterson and J. L. Hennessy, Computer Architecture: A Quantitative Approach, 6th ed. Morgan Kaufmann, 2017.

- [10] IBM. (n.d.). IBM Z and LinuxONE. Retrieved from https://www.ibm.com/it-infrastructure/z

- [11] IBM. (n.d.). z/OS Operating System. Retrieved from https://www.ibm.com/it-infrastructure/z/capabilities/zos

- [12] IBM. (n.d.). z/VM Virtualization. Retrieved from https://www.ibm.com/it-infrastructure/z/capabilities/zvm

- [13] IBM. (n.d.). Linux on IBM Z. Retrieved from https://www.ibm.com/it-infrastructure/linux-on-z

- [14] US-CERT. (2020, December 13). AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations. Retrieved from https://us-cert.cisa.gov/ncas/alerts/aa20-352a

- [15] Krebs, B. (2020, December 14). SolarWinds: What Hit Us Could Hit Others. Retrieved from https://krebsonsecurity.com/2020/12/solarwinds-what-hit-us-could-hit-others/

- [16] Cisco. (n.d.). Patch Management. Retrieved from https://www.cisco.com/c/en/us/products/security/patch-management.html