Configuring NAS and Mapping Network Shares

Role-Based Drive Access via AD Integration

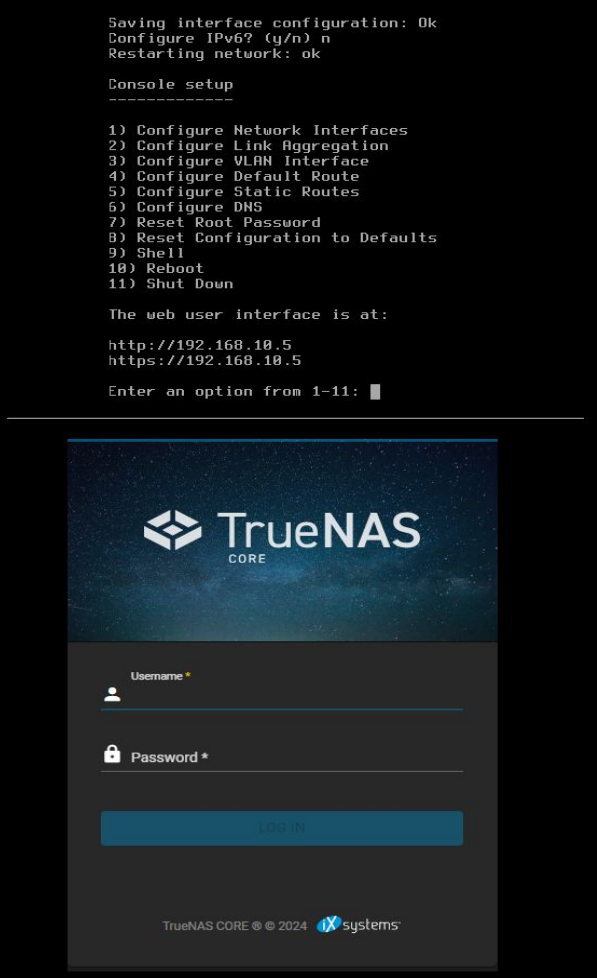
By Miguel K.

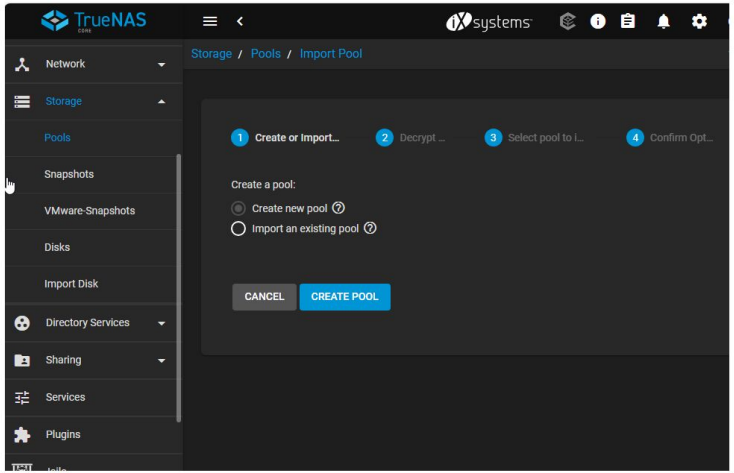
Setting Up a Virtual NAS with Active Directory Integration and SMB Sharing

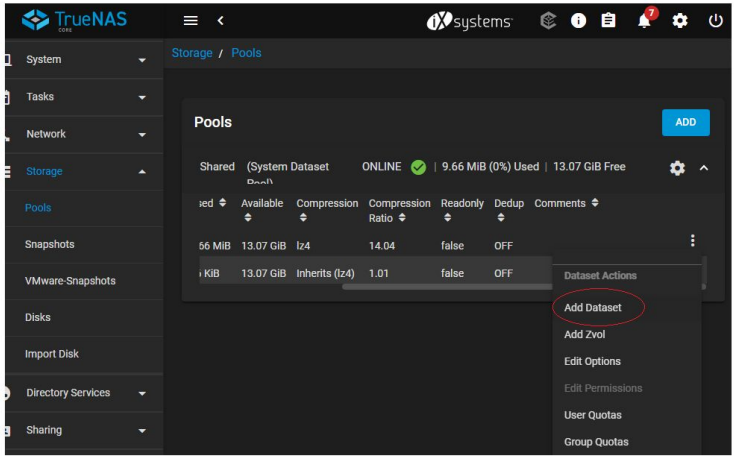
In this project, I configured a virtual NAS using TrueNAS, integrated it into my Active Directory network, and assigned a static IP address to the interface. I created a storage pool and SMB share, allowing seamless file sharing across the network. Active Directory integration enabled role-based access to the shared network drives by creating and managing user groups within AD. The project concluded with successfully mapping the network drives on Windows and ensuring proper file and folder access based on AD group permissions.

Configuring TrueNAS VM in a Virtual Network

- I began by installing the TrueNAS ISO and setting up a virtual machine for the NAS configuration.
- Next, I configured a **static IP address** for the TrueNAS VM within my virtual network to ensure it was on the same network as my Active Directory domain.
- Finally, I accessed the **TrueNAS web interface**,as shown in the screenshot, where I could manage the storage and configuration settings.





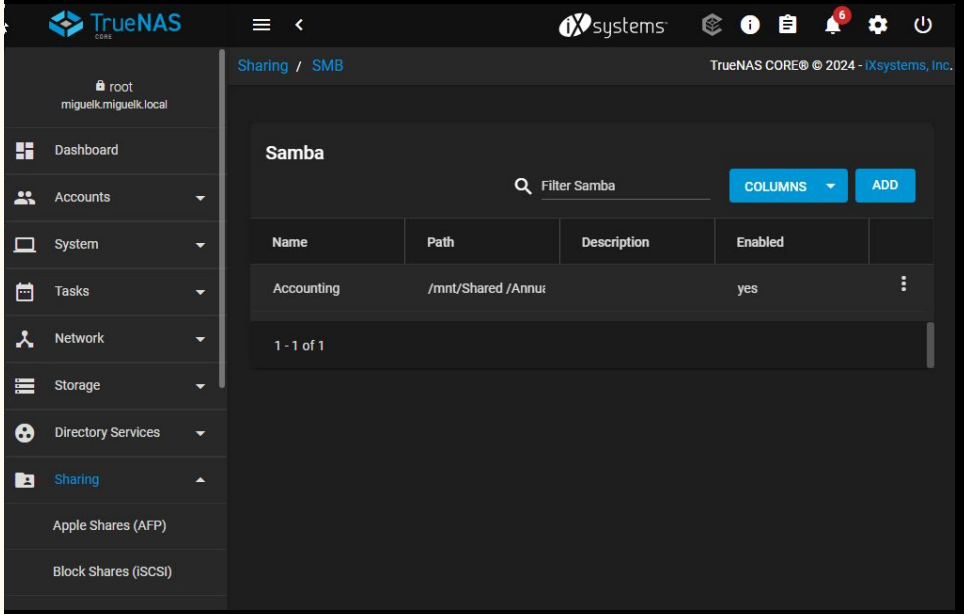


Creating Storage Pool and Dataset

- I created a storage pool in TrueNAS to allocate disk space for data storage.
- I then created a dataset within the storage pool to organize and manage data efficiently.
- This setup prepares the environment for integration with Active Directory and file sharing.

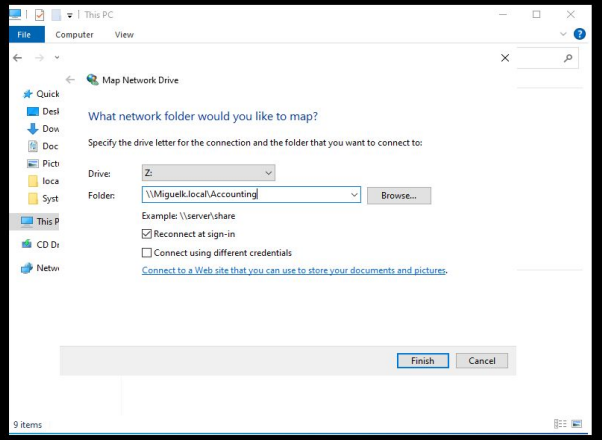
Setting Up the Accounting Share

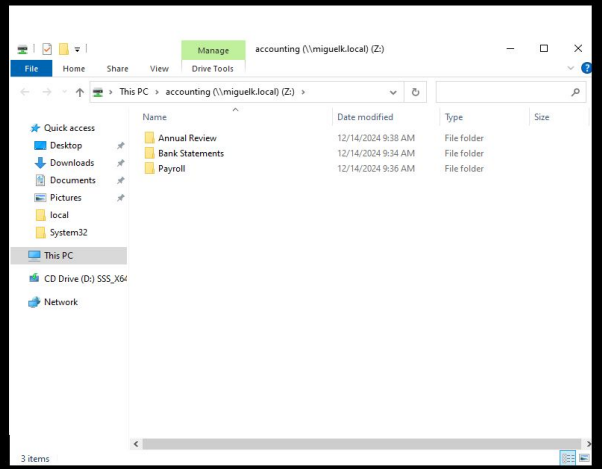
- Set up an SMB share named **Accounting** in TrueNAS to enable file sharing within my network.
- I created this share to establish a centralized location for secure file access and integrated it with Active Directory.
- In the next slide, I will map to the Accounting share.



Mapping Network Drives

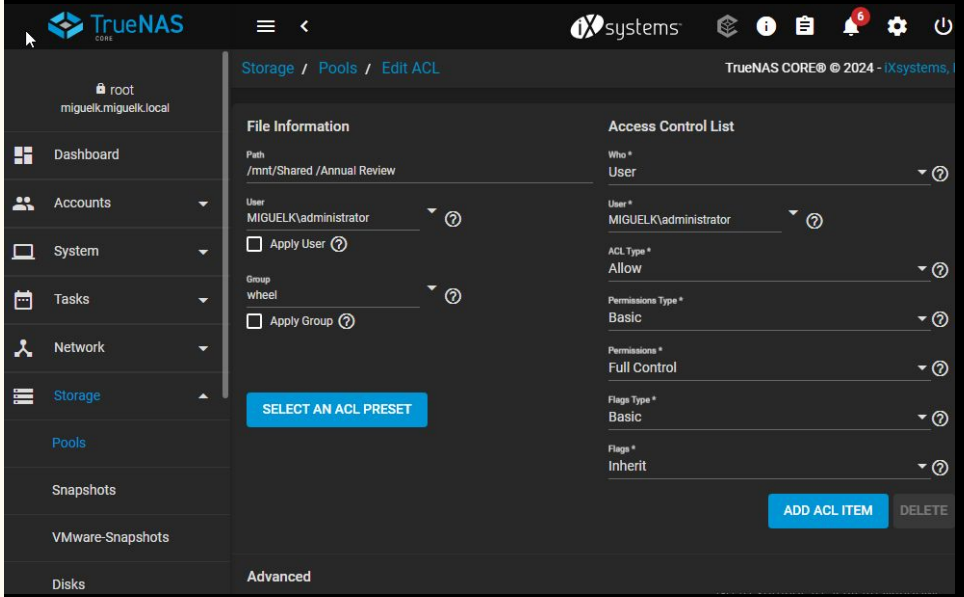
- I configured a DNS entry in Active Directory to map the TrueNAS server's IP address to the hostname **Miguelk.local** by creating an A Record under the Forward Lookup Zones.
- I mapped the **Accounting** SMB share in TrueNAS to demonstrate accessing shared network resources for collaboration..
- Once mapped, the shared network folders become accessible to users with the appropriate permissions, as shown in the image.

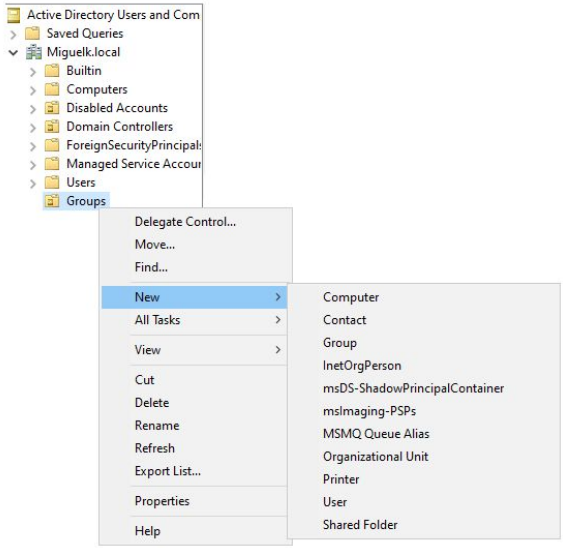


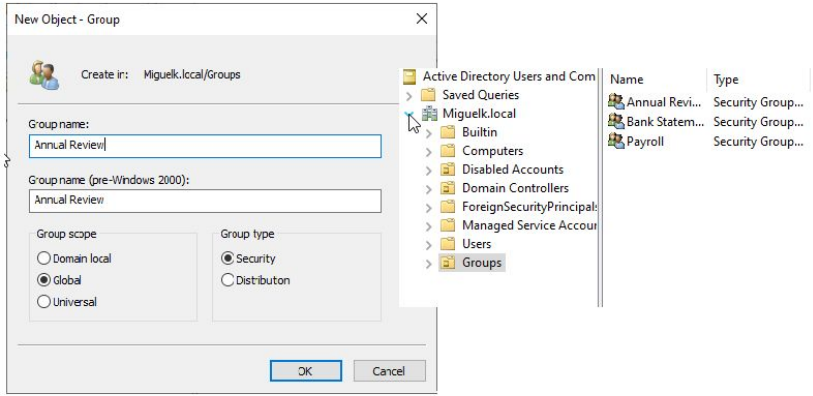


Configuring ACL Rules

- I implemented an **ACL rule** within the TrueNAS interface to manage permissions for the Accounting dataset.
- By integrating Active Directory with TrueNAS, I assigned **administrative control** to the Active Directory Administrator for managing access.
- In the next slide, I will configure folder access based on Active Directory groups.

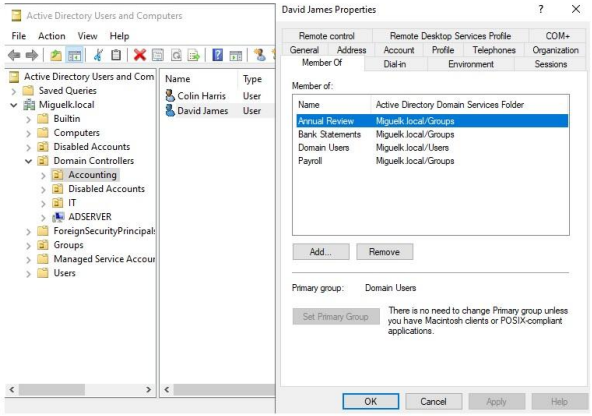


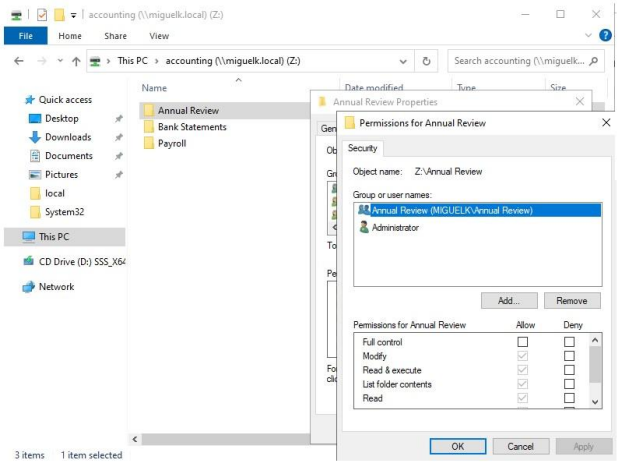




Creating Security Groups for Folder Permissions

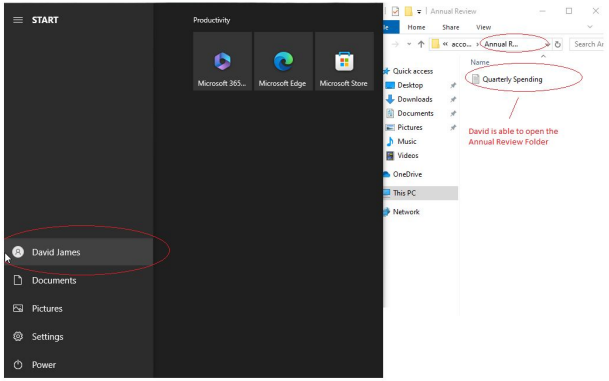
- I created groups in Active Directory to gain granular control over folder access within my network share.
- Each group I created will be assigned to a specific folder in the Accounting share in the next slide.
- This approach ensures that only authorized users, based on group membership, can access the designated folders.

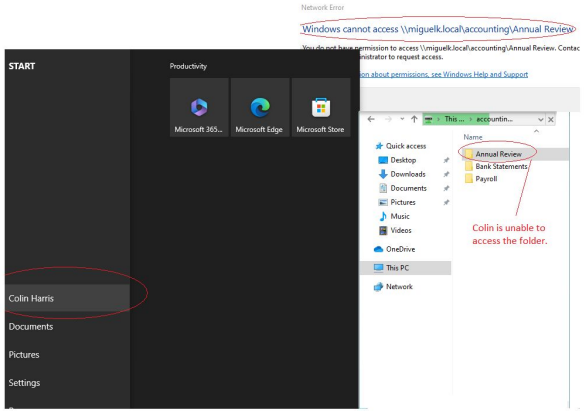




Configuring Folder Access

- I added a user (David James) to the security groups created in the previous slide.
- I linked the security groups to specific folders to restrict access to users within those groups.
- With the security group granted access to the folder and the user added to the group, the user now has permission to access the folder.





Role-Based Access

- I added David James to the Annual Review group, granting him access to the folder, as shown in the image.
- Colin Harris was not added to the group, so he cannot access the folder, as shown in the image.
- As the administrator, I can manage role-based folder access to secure the network and protect data.

Project Summary

- In this project, I set up a virtual NAS using TrueNAS and integrated it with Active Directory to enable secure, role-based access to shared files.

- I configured a static IP address, created a storage pool, and set up an SMB share named Accounting to centralize file sharing across the network. By creating and managing security groups in Active Directory, I established granular control over folder permissions, ensuring only authorized users could access specific folders.

- The project concluded with mapping network drives and verifying access controls, showcasing a seamless and efficient file-sharing solution.

- This setup highlights essential components of enterprise IT infrastructure, emphasizing network security and role-based access for effective collaboration and data protection.