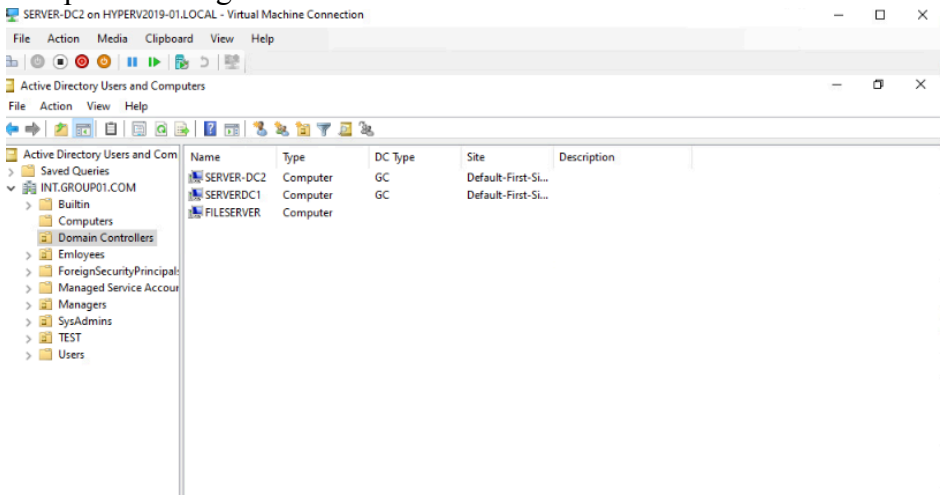
Critical Section

Establish Organization Overview

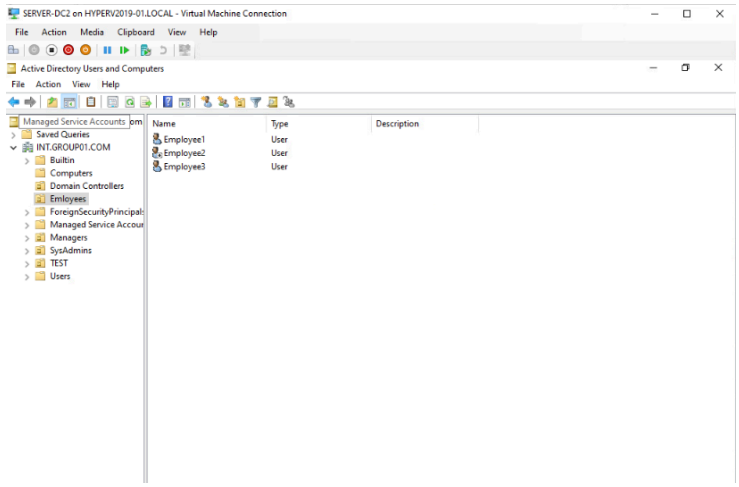
We created a small organization, a company with managers, employees, and administrators (hr/it). In this organization, each department has its own OU with group assignments and 3 users each. They have 2 workstations each and a network drive with 3 folders. We created a file server with cloud back up and are using our main server (SERVER-DC2) as a router for the workstations. Our departments are on their own VLANs as well as our servers. We are using Windows defender and firewall for security, have enable file monitoring and logs as well as user authentication. We also have snapshot schedules, AWS Cloud service, and created RTO. The details are listed below:

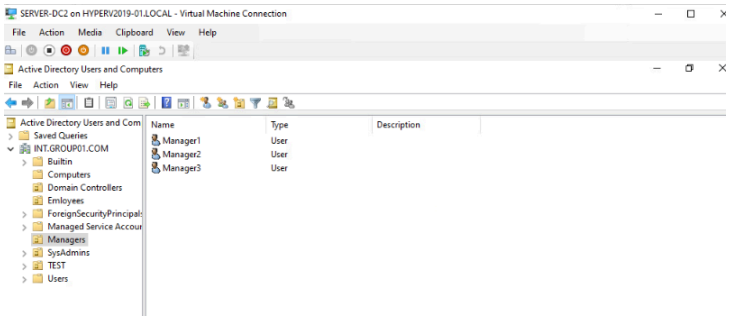
Event	Identifier	Progress
Company Name: **Company Type:**	ImagineGraphics Small Marketing/graphic design	
Workstations ***Min 2** ***Win10, 8.1, or Linux**	1.Admin Office-01 2. Admin Office-02 3. Managerswks1 4. Managerswks2 5. Employeeswks1 6. Employeeswks2	Complete
Windows Servers ***Min 2** ***2022/2025**	1.SERVER-DC2 (Main) 2. File Server 3. ServerDC1(backup server)	Complete
Organizational Units ***Min 3 OUs** ***3 users per OU** ***Shared folder for each OU**	1.sysAdmins 2.Managers 3.Employees Folders:	Complete
Router/Firewall ***Integrated**	Windows Defender Enabled Across all machines	Complete
Active Directory Domain Controller	SERVER-DC1	Complete
Hyper-V Type 1	Installed in Folder - Critical Section Group01	Complete

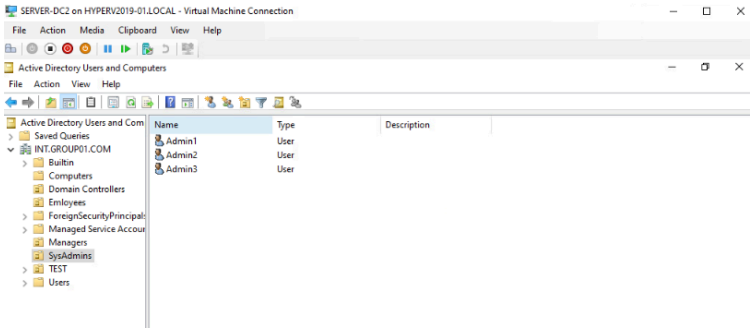
Completed configuration of our servers:



Added OU's and groups and users for each department and system. Each group member is enabled on their corresponding machines:

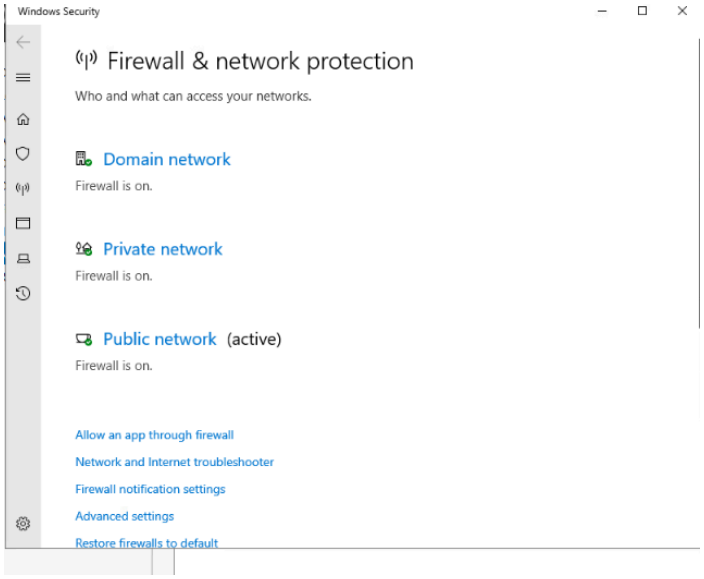






Security Plan

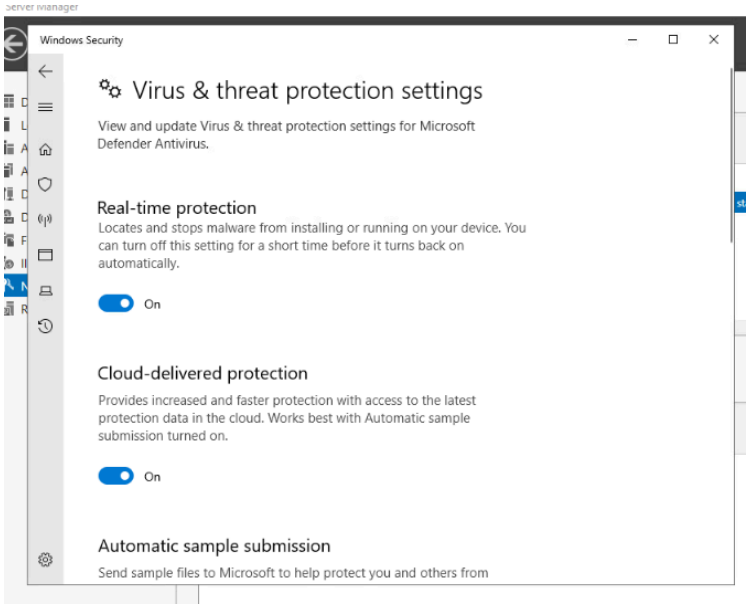
Firewall Windows Fall enabled across machines:



User authentication

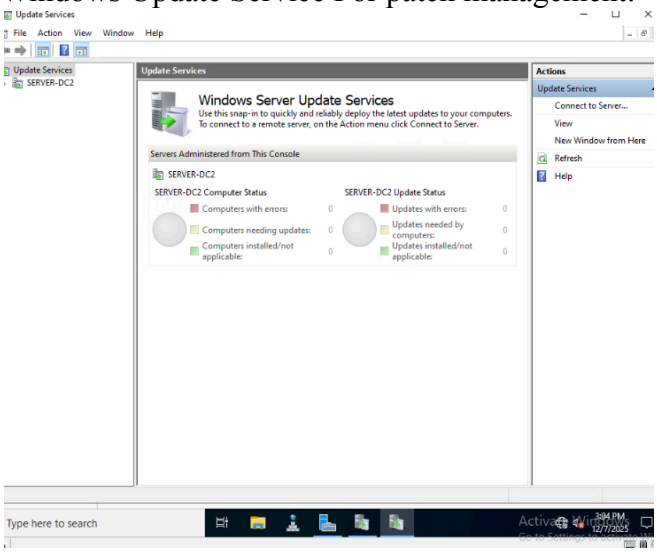
- Created User accounts for existing Employees. Employees must reset their Passwords immediately upon first log in
- Each member has a separate log in to access resources and limit misuse through multiuser accounts.

Antivirus Windows defender enabled across all machines:



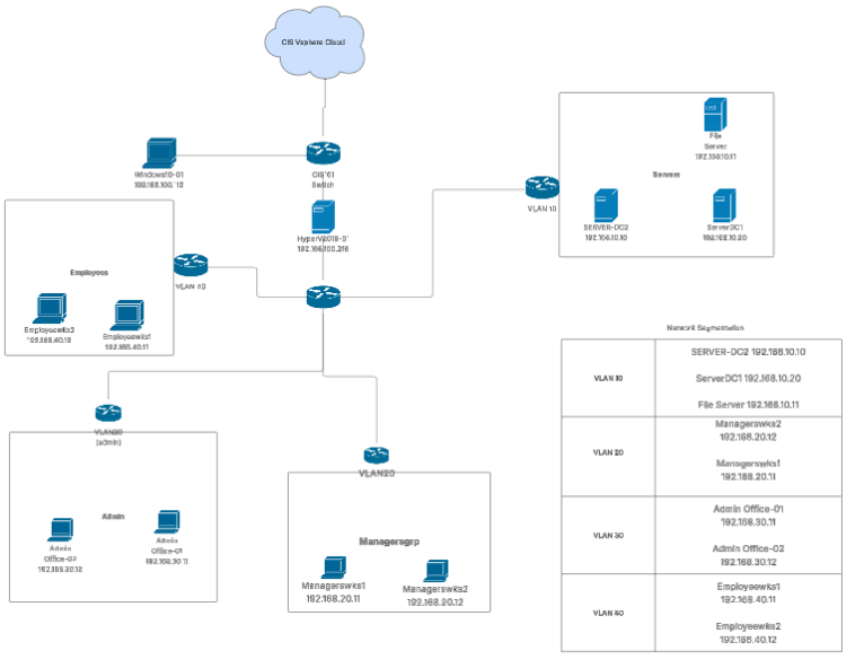
€ Patch Management

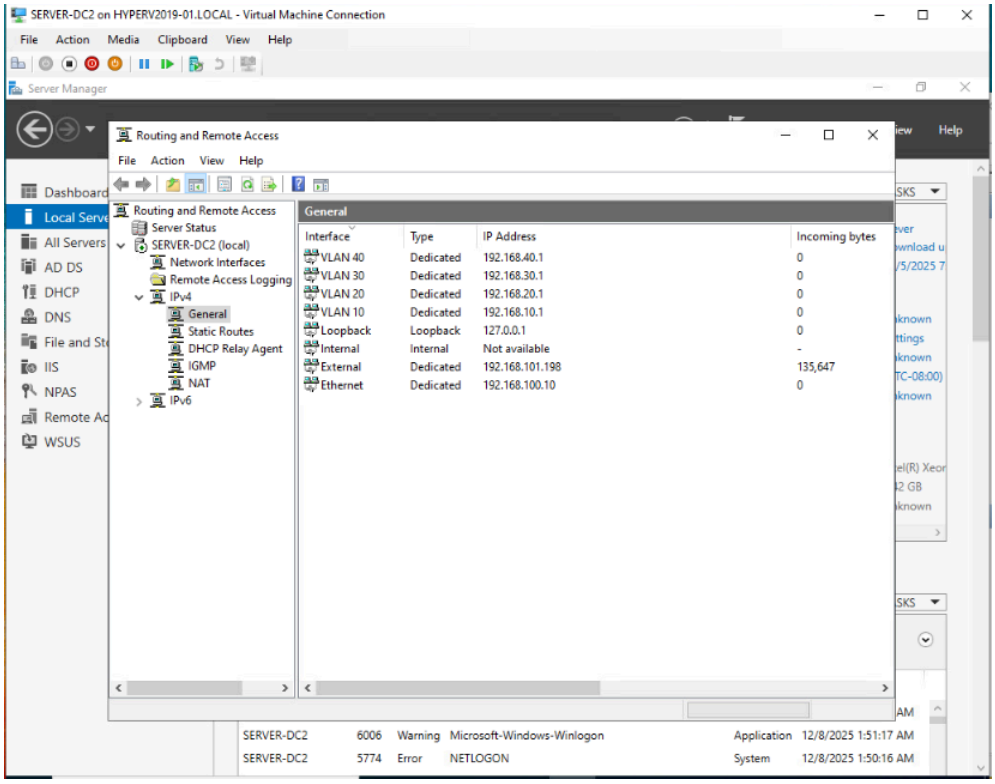
Windows Update Service For patch management:



Topology Diagram

Topology diagram includes the network segmentation details:



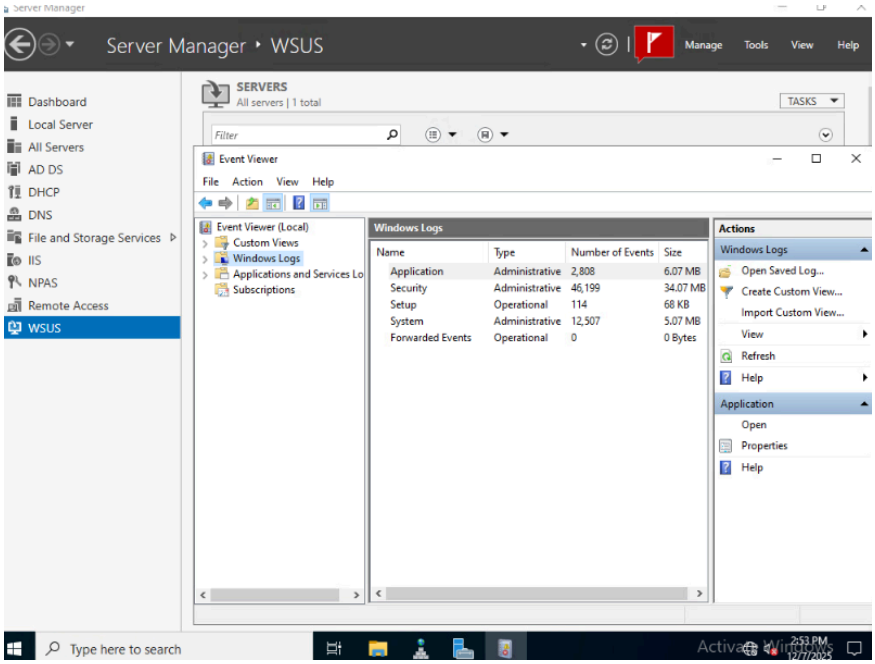


Created internally on DC2, using a trunk and 4 VLANs

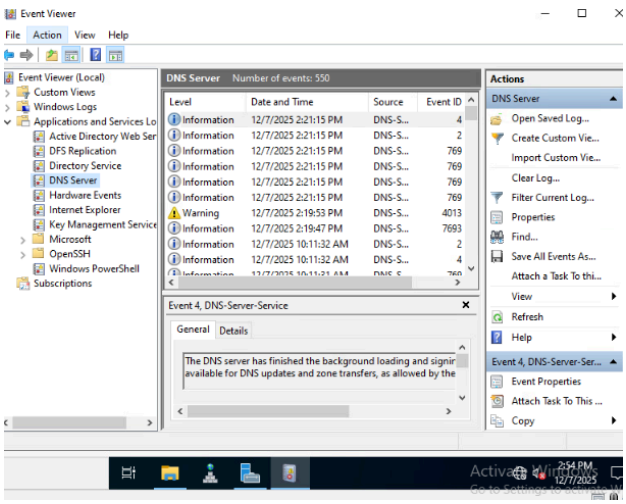
File Monitoring

Through the use of Event View and enabling File Auditing in Group Policy Management Editor, we have:

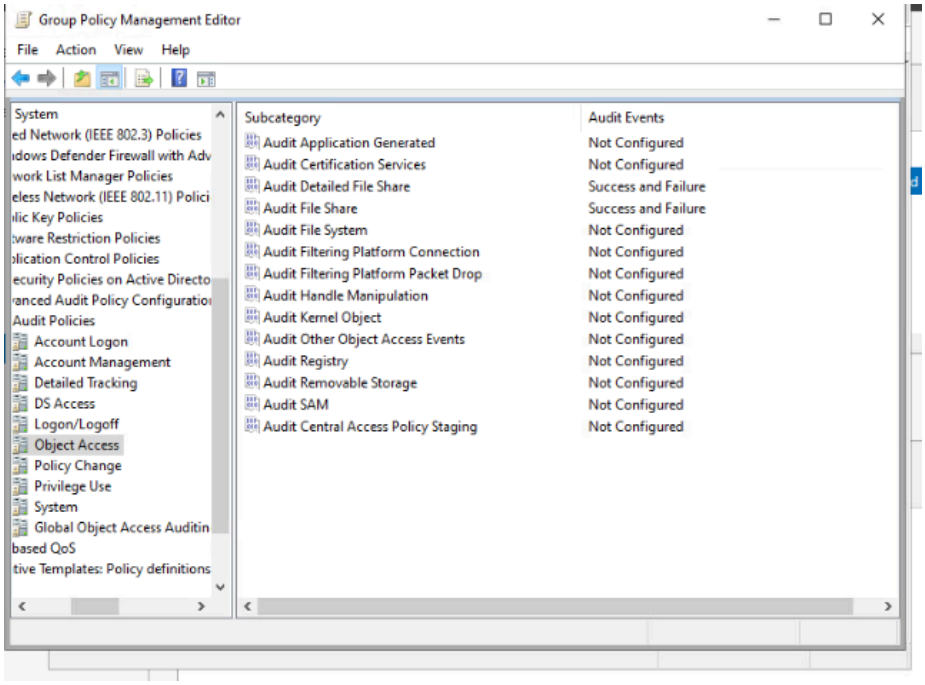
Event Logs

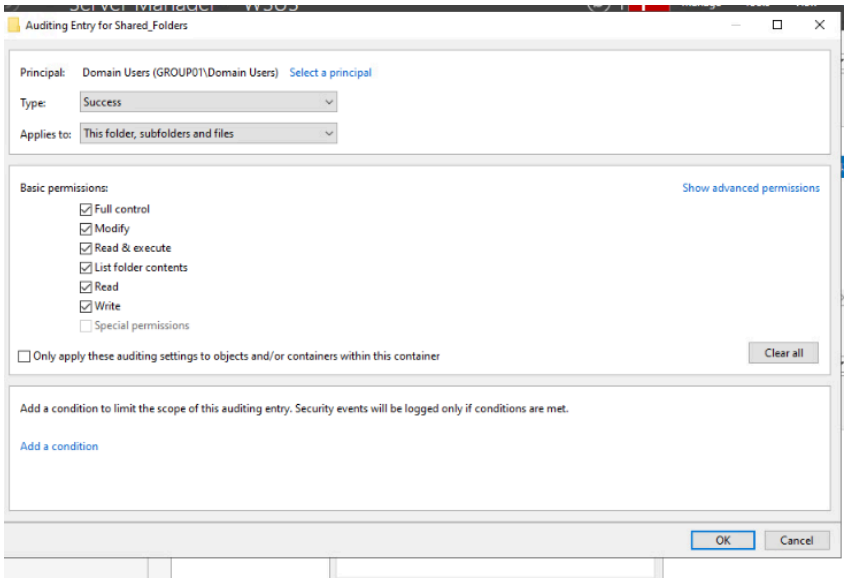


DHCP/DNS logs



File Access on shared folders





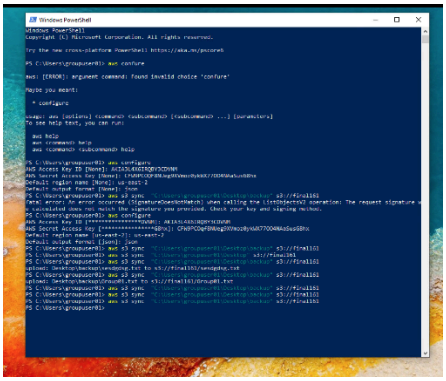
Folders and their Purpose:

The separate departments were given 3 folders each and their own respective drives:

Shared Folder	Drive	Access	Purpose
Logos 2025	\\FileServer\Graphics	Employees	Employee specific folder for shared materials
Logo Tees	\\FileServer\Graphics	Employees	Employee specific folder for shared materials
Holiday Advt	\\FileServer\Graphics	Employees	Employee specific folder for shared materials
Promotions	\\FileServer\Managers	Managers	Managerial files
Sales	\\FileServer\Managers	Managers	Managerial files
Training	\\FileServer\Managers	Managers	Managerial files
Employee Log	\\FileServer\Admins	Admin	Admin/support files
Payroll	\\FileServer\Admins	Admin	Admin/support files
Timesheets	\\FileServer\Admins	Admin	Admin/support files

Back up and Disaster Recovery Plan

Snapshot schedules
Onsite and offsite storage solutions
Cloud back up information
Recovery time objectives RTO and RPO

Plan	Completed
Snapshot schedules	Checkpoints created for the VMs
Storage	File Server with backup to AWS
Cloud	Connected to AWS 
RTO/RPO	AD, DNS, FileServer objective to recover time is 4 hours For all clients, 12 hours