File Sharing Services Implementation

Overview

Extended the Active Directory domain implementation to include File and Print Services, demonstrating enterprise-level file sharing capabilities with proper security controls and network accessibility.

Implementation Objectives

- **Centralized File Storage:** Establish network-accessible shared folders
- **Security Implementation**: Configure dual-layer permission model (Share + NTFS)
- **Domain Integration**: Leverage Active Directory for access control
- **Client Access**: Validate file sharing from domain-joined clients
- **Best Practices:** Implement principle of least privilege and layered security

Technical Implementation

Phase 1: File Services Role Configuration

Server Preparation

- Verified File and Print Services role availability on Windows Server 2022
- Confirmed Active Directory integration for user authentication
- Validated network connectivity between server and domain clients

Phase 2: Shared Folder Creation and Configuration

2.1 Folder Structure Setup

```
C:\Shared\
├── Created base shared folder on local disk
├── Established logical naming convention
└── Prepared for network sharing configuration
```

2.2 Share-Level Permissions Configuration

- **Access Method**: Properties → Sharing → Advanced Sharing
- **Share Name**: "Shared" (customizable based on business requirements)
- **Network Sharing**: Enabled "Share this folder" for network accessibility
- **Permission Scope**: Domain Users group (enterprise-wide access)
- **Access Level**: Read-only (implementing least privilege principle)
- **Security Model**: Domain-integrated authentication

2.3 NTFS Permissions Configuration

- **Access Method**: Properties → Security Tab
- **Permission Layer**: File system level security (more granular than share permissions)
- **User/Group Management**: Domain Users with appropriate NTFS rights
- **Advanced Features**:
  - Individual user permission assignment capability
  - Time-based access control potential
  - Inheritance and special permissions management
  - Audit trail configuration options

Phase 3: Permission Architecture

Dual-Layer Security Model

```
Network Access (Share Permissions)
├── Controls who can access the share over the network
├── Applied at the share level
├── Domain Users: Read access
└── Simpler permission set (Read, Change, Full Control)

File System Access (NTFS Permissions)
├── Controls detailed file and folder access
├── Applied at individual file/folder level
├── More granular permission options
├── Supports inheritance and special permissions
└── Enables user-specific and temporary access grants
```

Permission Interaction

- **Effective Permissions**: Most restrictive between Share and NTFS applies
- **Network Access**: Requires both Share and NTFS permissions
- **Local Access**: Only NTFS permissions apply (direct server access)

Security Implementation

Access Control Strategy

Principle of Least Privilege

- Default permissions set to Read-only for Domain Users
- Full Control reserved for administrative accounts
- Change permissions granted based on business requirements

Granular Permission Management

- NTFS permissions enable individual user access grants
- Temporary access can be configured for specific business needs
- Executive or management special access requests accommodated through NTFS layer

Audit and Compliance

- File access events logged through Windows Event Log
- Permission changes tracked for compliance reporting
- Active Directory integration provides centralized audit trail

Testing and Validation

Connectivity Testing

Server-Side Validation

- Verified shared folder appears in network shares
- Confirmed share permissions apply to domain users
- Validated NTFS permissions function correctly

Client-Side Testing

- Domain-joined clients can discover shared folders
- Network path accessibility: `\\ServerName\Shared`
- User authentication through domain credentials
- Read access functioning as configured
- Write restrictions properly enforced

Permission Verification

- **Share Permissions**: Domain Users have network access
- **NTFS Permissions**: File system security properly layered
- **Effective Access**: Combined permissions work as intended
- **Security Boundaries**: Unauthorized access properly restricted

Business Applications

Collaboration Enhancement

- **Centralized Storage**: Single location for shared business documents
- **Version Control**: Central file storage reduces version conflicts
- **Access Management**: IT can control who accesses what resources
- **Backup Integration**: Centralized files easier to backup and protect

Operational Benefits

- **Reduced IT Support**: Centralized file access reduces support tickets
- **Scalability**: Easy to add new users and adjust permissions
- **Security**: Consistent security policy enforcement
- **Compliance**: Centralized audit and control capabilities

Advanced Configuration Options

Extended Permission Scenarios

Executive Access Example

```
Scenario: Company president needs temporary full access to confidential folder
Solution: Add individual user to NTFS permissions with Full Control
Duration: Time-limited through manual management or automated tools
Security: Maintains audit trail of executive access
```

Department-Specific Shares

```
Structure: Multiple shared folders for different departments
Permissions: Department-specific security groups
Management: OU-based group policy application
Scalability: Easy addition of new departments and users
```

Integration Possibilities

- **DFS (Distributed File System)**: Multi-server file sharing
- **File Server Resource Manager**: Quotas and file screening
- **Shadow Copies**: Previous versions and backup integration
- **BranchCache**: Optimized file access for remote locations

Troubleshooting Procedures

Common Issues and Resolutions

Network Access Problems

- **Issue**: Clients cannot access shared folders
- **Diagnosis**: Check network connectivity and DNS resolution
- **Resolution**: Verify client DNS points to domain controller
- **Prevention**: Maintain proper network configuration documentation

Permission Conflicts

- **Issue**: Users have unexpected access levels

- **Diagnosis**: Review both Share and NTFS permissions
- **Resolution**: Adjust more restrictive permission layer
- **Best Practice**: Document permission inheritance rules

Authentication Failures

- **Issue**: Domain users cannot authenticate to shares
- **Diagnosis**: Verify Active Directory connectivity
- **Resolution**: Check domain trust relationships and time synchronization
- **Monitoring**: Enable detailed authentication logging

Skills Demonstrated

Technical Competencies

- **File Services Administration**: Windows Server file sharing configuration
- **Permission Management**: Dual-layer security model implementation
- **Active Directory Integration**: Domain-based access control
- **Network Services**: SMB/CIFS protocol understanding
- **Security Architecture**: Layered security approach
- **Troubleshooting**: Systematic problem resolution methodology

Enterprise Skills

- **Business Analysis**: Understanding file sharing business requirements
- **Security Planning**: Risk-based permission assignment
- **Documentation**: Comprehensive technical documentation
- **Change Management**: Structured implementation approach
- **Compliance Awareness**: Audit trail and access control importance

Future Enhancements

Scalability Improvements

- **DFS Implementation**: Distributed file system for high availability
- **File Classification**: Automated file management based on content
- **Quota Management**: Storage limit enforcement per user/department
- **Advanced Auditing**: Detailed file access monitoring and reporting

Security Enhancements

- **File Encryption**: EFS or BitLocker integration for sensitive data
- **Data Loss Prevention**: File screening and content inspection
- **Advanced Permissions**: Claims-based access control implementation

- **Backup Integration**: Automated backup of shared folder contents

---

Conclusion

This comprehensive Windows Server infrastructure project successfully demonstrates enterprise-level skills essential for modern IT environments. The implementation showcases proficiency in:

Core Infrastructure Services

- Active Directory domain controller deployment and management
- DNS services configuration and integration
- File and Print Services with enterprise-grade security
- Client-server integration and management

Security and Compliance

- Dual-layer permission model (Share + NTFS permissions)
- Group Policy implementation and enforcement
- Domain-integrated access control and authentication
- Audit trail establishment and security monitoring

Professional Competencies

- Systematic project implementation methodology
- Comprehensive testing and validation procedures
- Enterprise-standard documentation practices
- Troubleshooting and problem resolution skills

The project provides a solid foundation for enterprise Windows environments while demonstrating the technical and professional skills required for system administrator, network administrator, and infrastructure engineer roles. The combination of Active Directory services and File Sharing capabilities shows practical understanding of how enterprise IT services integrate to support business operations.

This project serves as concrete evidence of hands-on experience with core Windows Server technologies, security implementation, and enterprise service management, making it an excellent portfolio piece for IT career advancement in Windows-focused environments.

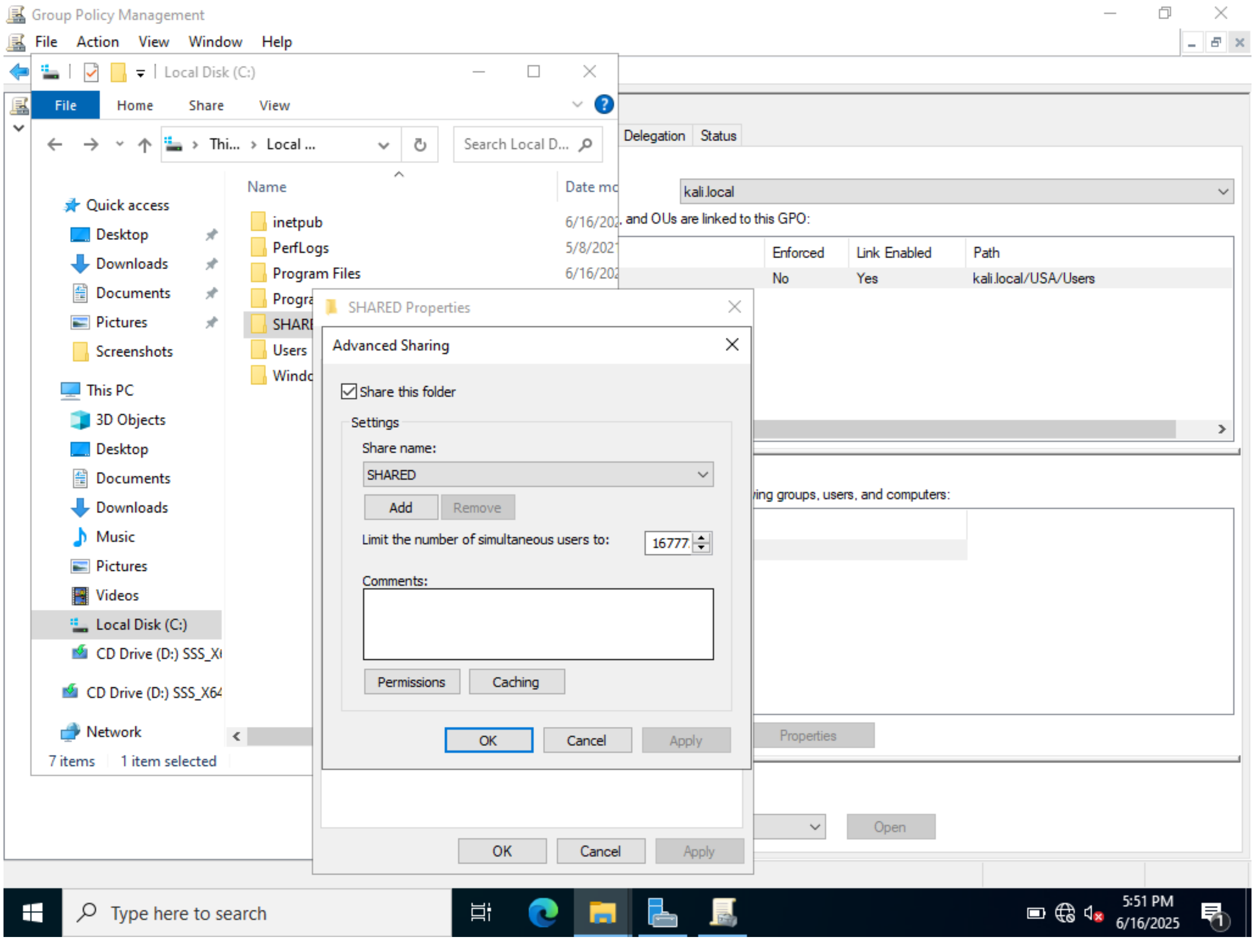
Appendix

Configuration References

- **Domain Controller IP**: 192.168.1.128 (example)
- **Domain Name**: kali.local (example)
- **DNS Servers**: 127.0.0.1 (primary), 8.8.8.8 (secondary)
- **OU Structure**: Domain → USA → Users/Computers
- **Shared Folder Path**: C:\Shared (server-side)
- **Network Share Path**: \ServerName\Shared
- **Share Permissions**: Domain Users (Read)
- **NTFS Base Permissions**: Domain Users (Read & Execute)

Command References

- **DNS Testing:** `nslookup domain.local`
- **Connectivity:** `ping domain-controller-ip`
- **Group Policy:** `gpupdate /force`
- **IP Configuration:** `ipconfig /all`
- **Network Shares:** `net view \\servername`
- **Share Access:** `\\servername\sharename`
- **Permission Testing:** `icacls foldername /T`



Name	Date mo
inetpub	6/16/202
PerfLogs	5/8/2021
Program Files	6/16/202
Progra	
SHARI	
Users	
Windo	

kali.local

and OUs are linked to this GPO:

	Enforced	Link Enabled	Path
	No	Yes	kali.local/USA/Users

ving groups, users, and computers:

Advanced Sharing

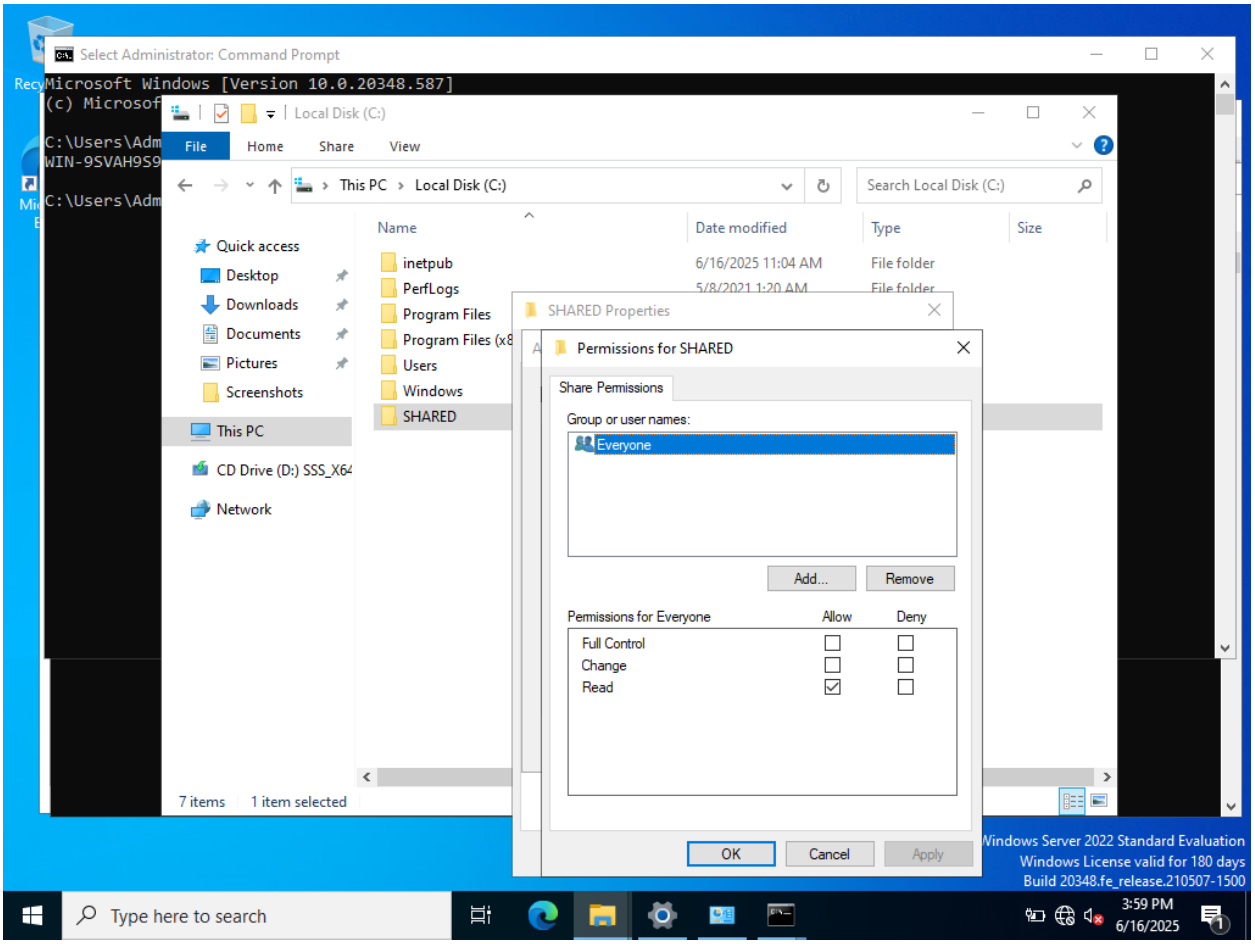
☑ Share this folder

Settings

Share name: SHARED

Limit the number of simultaneous users to: 16777

Comments:



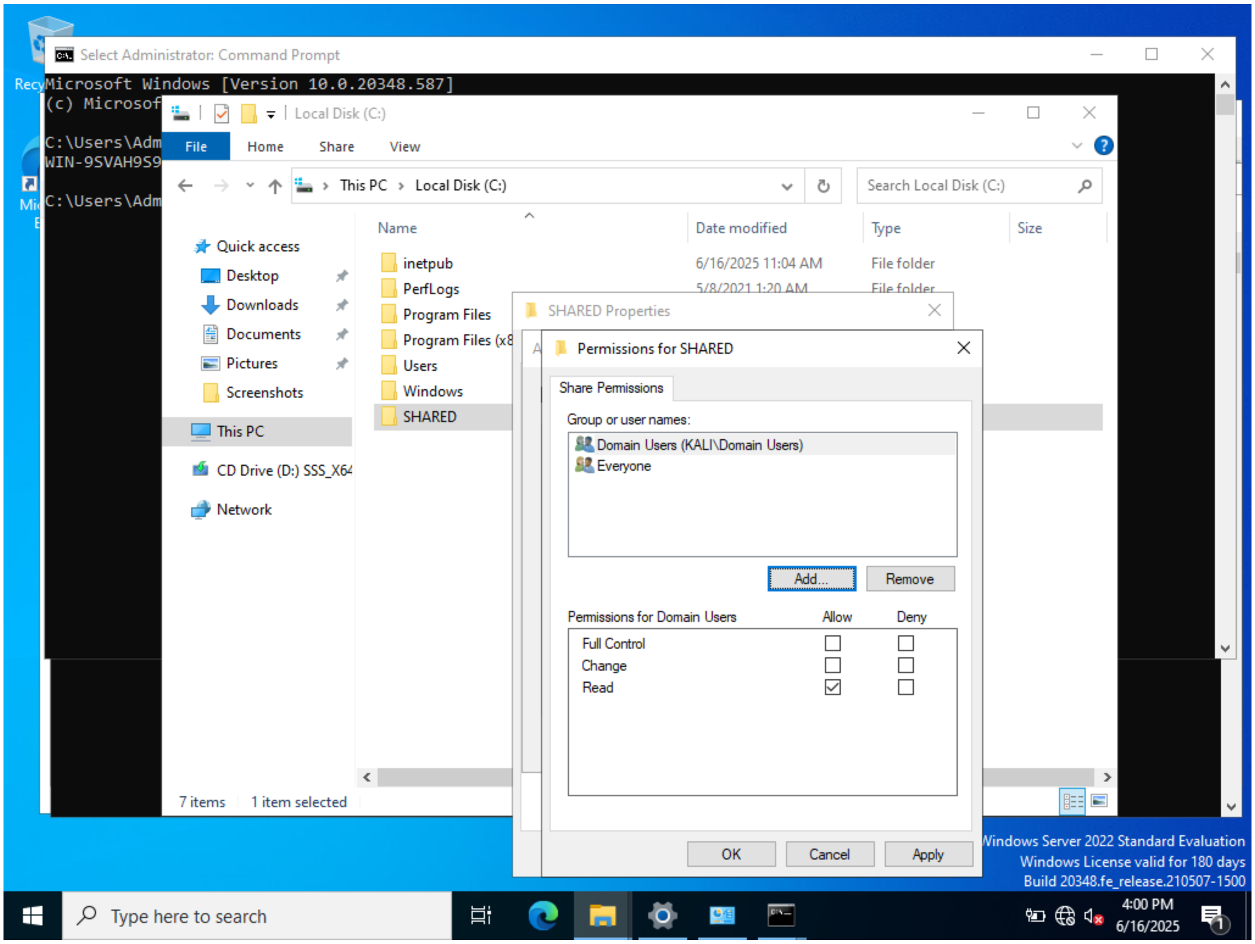
```
Microsoft Windows [Version 10.0.20348.587]
(c) Microsof

C:\Users\Adm
WIN-9SVAH9S9

C:\Users\Adm
```

Name	Date modified	Type	Size
inetpub	6/16/2025 11:04 AM	File folder	
PerfLogs	5/8/2021 1:20 AM	File folder	
Program Files			
Program Files (x8			
Users			
Windows			
SHARED			

Group or user names:

Everyone

Permissions for Everyone	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□



```
Microsoft Windows [Version 10.0.20348.587]
(c) Microsof

C:\Users\Adm
WIN-9SVAH9S9

C:\Users\Adm
```

Name	Date modified	Type	Size
inetpub	6/16/2025 11:04 AM	File folder	
PerfLogs	5/8/2021 1:20 AM	File folder	
Program Files			
Program Files (x8			
Users			
Windows			
SHARED			

7 items 1 item selected

Permissions for SHARED

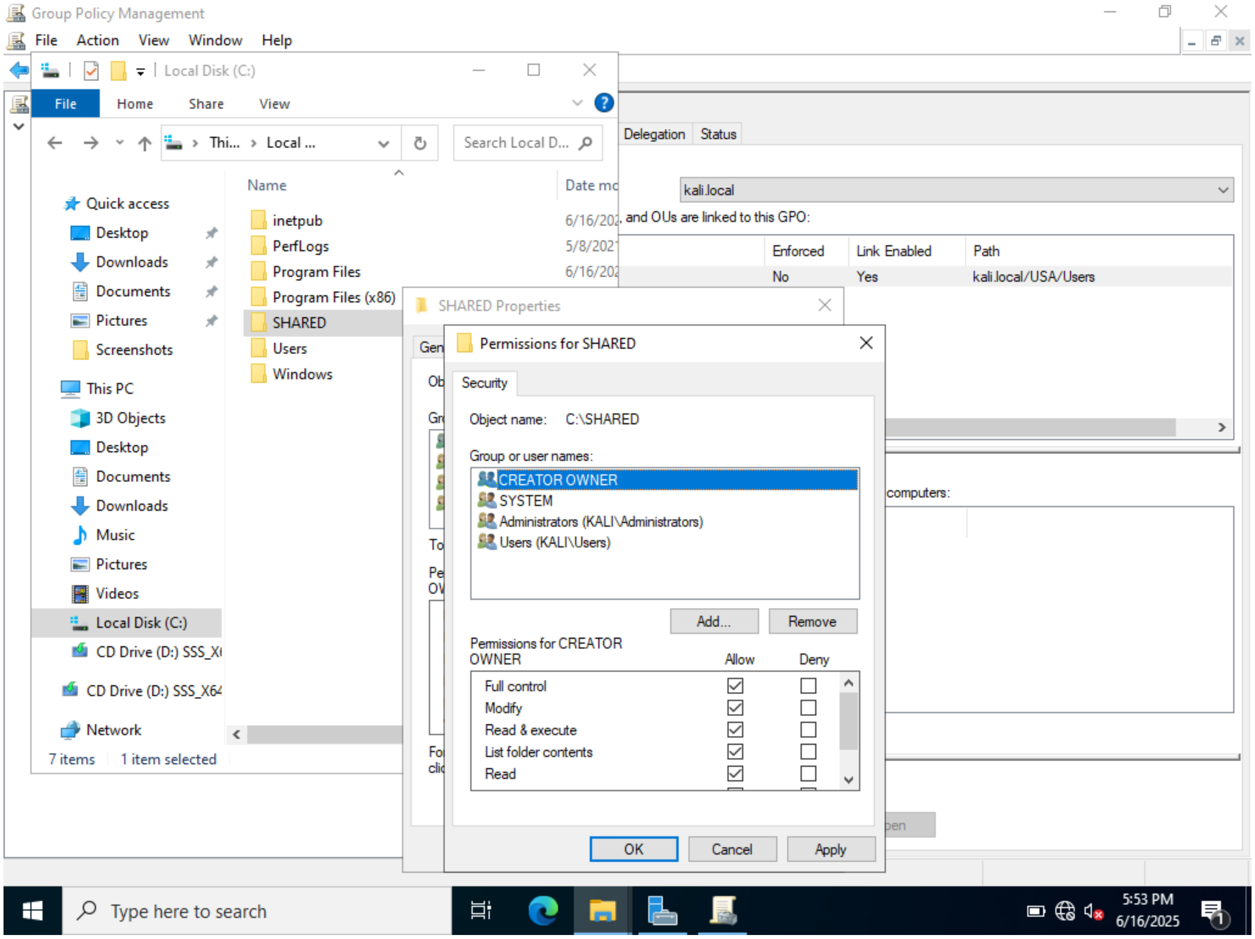
Share Permissions

Group or user names:

- Domain Users (KALI\Domain Users)
- Everyone

Permissions for Domain Users	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□

Windows Server 2022 Standard Evaluation
Windows License valid for 180 days
Build 20348.fe_release.210507-1500



Name	Date mo
inetpub	6/16/202
PerfLogs	5/8/2021
Program Files	6/16/202
Program Files (x86)	
SHARED	
Users	
Windows	

kali.local

and OUs are linked to this GPO:

	Enforced	Link Enabled	Path
	No	Yes	kali.local/USA/Users

Object name: C:\SHARED

Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (KALI\Administrators)
- Users (KALI\Users)

Permissions for CREATOR OWNER	Allow	Deny
Full control	☑	□
Modify	☑	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□