From Zero to Hero

Beginner's Guide to Active Directory

Dale Hobbs

About Me

- Security Analyst at Black Hills Information Security
- Former Blue Teamer
- Certifications: CRTP, GSEC, GCIH, GCIA, GPEN, GCCC, GDAT

BLACK HILLS | Information Security

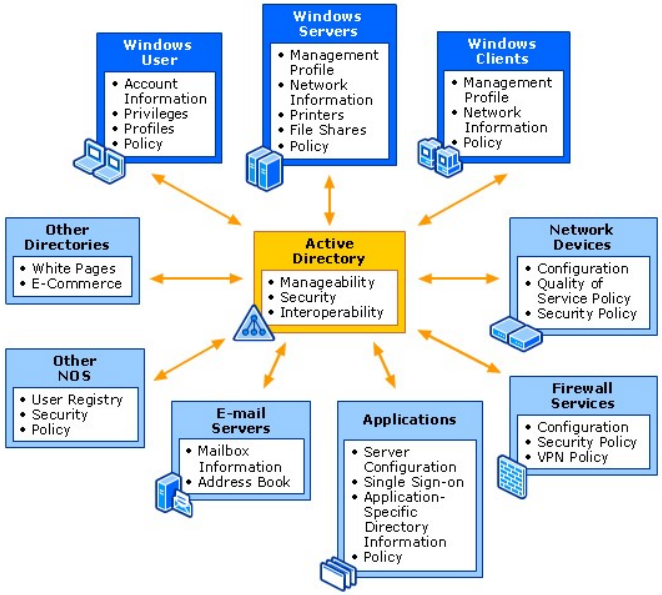
AGENDA

- What is Active Directory?
- AD Objects, Components and Architecture
- Replication, Trusts and Group Policy
- Authentication Protocols
- Users, Groups and Computers
- Active Directory Certificate Services (ADCS)
- Best Practices

BLACK HILLS | Information Security

What is Active Directory

- Directory service used to manage Windows environments
- Stores information about objects on the network
- Enables secure management of an entire network
- Highly scalable, supports millions of objects
- Many features are arguably not "secure by default" and can be easily misconfigured
- Around 95% of Fortune 500 companies run Active Directory



BLACK HILLS | Information Security

Key Benefits

- Centralized Identity Management
- Enhanced Security (Authentication and Authorization)
- Scalability
- Single Sign-On (SSO)
- Replication and Redundancy
- Delegation of Administration
- Simplified User and Resource Access

Active Directory Objects

- Users
- Contacts
- Computers
- Shared Folders
- Groups
- Organization Units (OUs)
- Domain
- Domain Controllers
- Sites

BLACK HILLS | Information Security

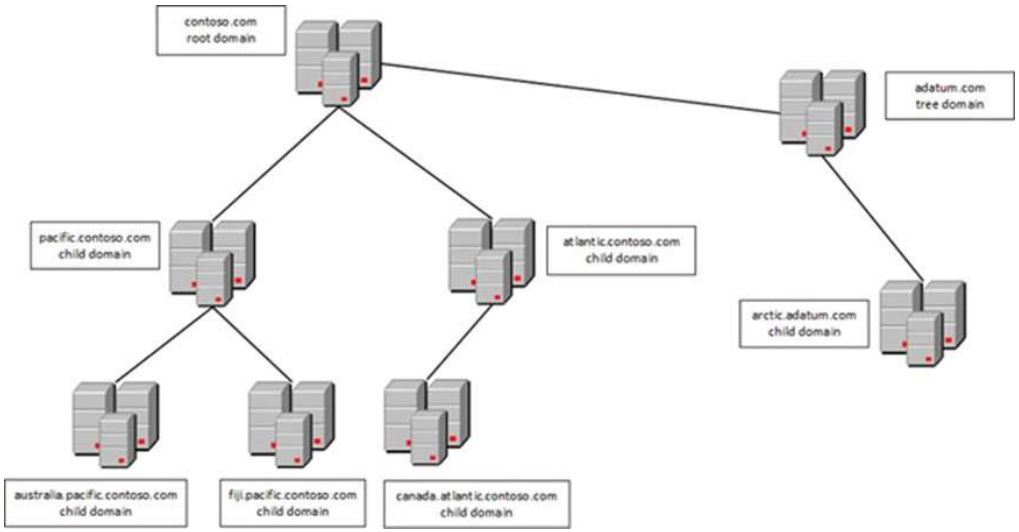
Active Directory Components

- Active Directory Domain Services (AD DS)
- Active Directory Lightweight Directory Services (AD LDS)
- Active Directory Federation Services (AD FS)
- Active Directory Certificate Services (AD CS)
- Active Directory Rights Management Services (AD RMS)

BLACK HILLS | Information Security

Active Directory Architecture

- Forests, Trees, and Domains
- Organizational Units (OUs)
- Sites and Subnets
- Domain Controllers
- Global Catalogs



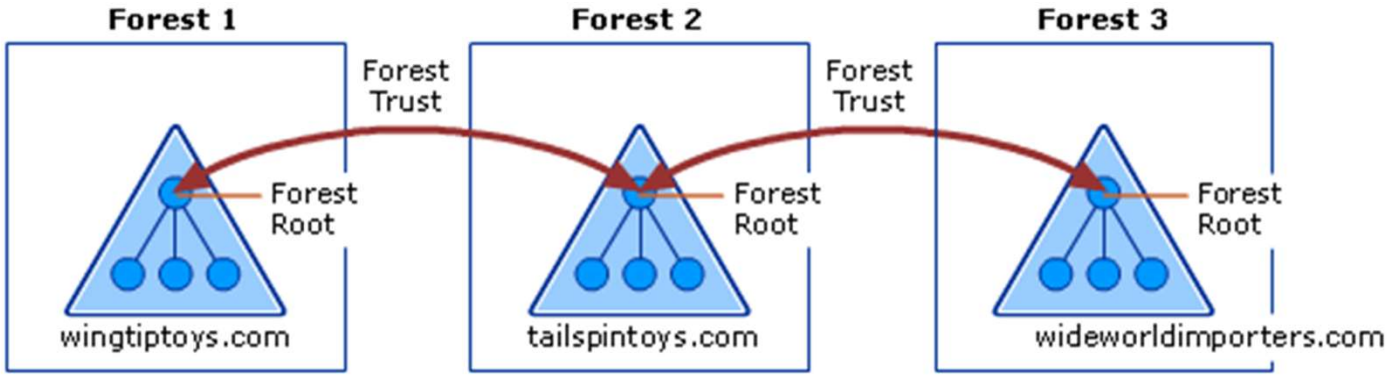
BLACK HILLS | Information Security

Active Directory Replication

- Synchronizes data between multiple DCs within a domain or forest.
- Facilitated by the Directory Replication Service
- Follows a specific replication topology
- Each DC has replication partners
- Replication occurs periodically based on predefined replication intervals
- Intra-Site Replication and Inter-Site Replication

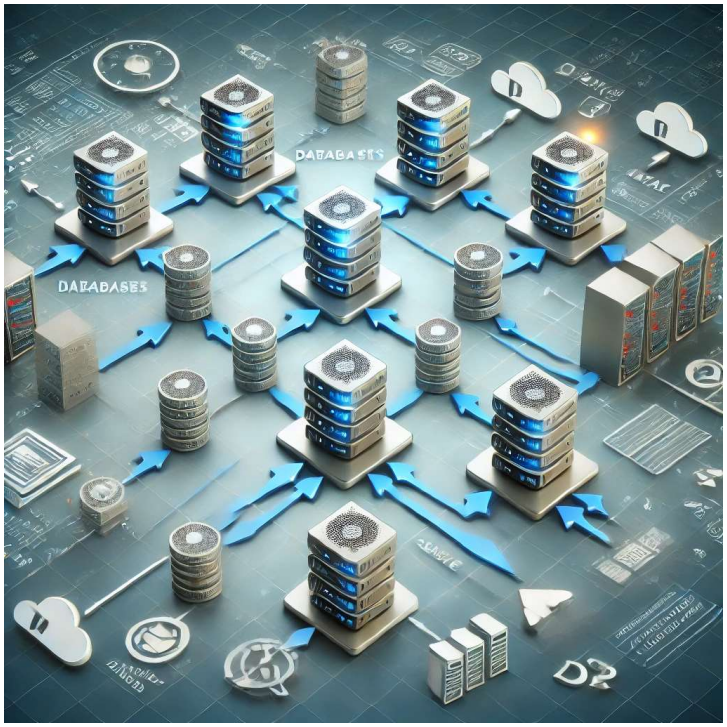
Trusts

- Enable users from one domain to access resources in another domain
- One-way
- Two-way
- Transitive
- Non-Transitive



AD Group Policy

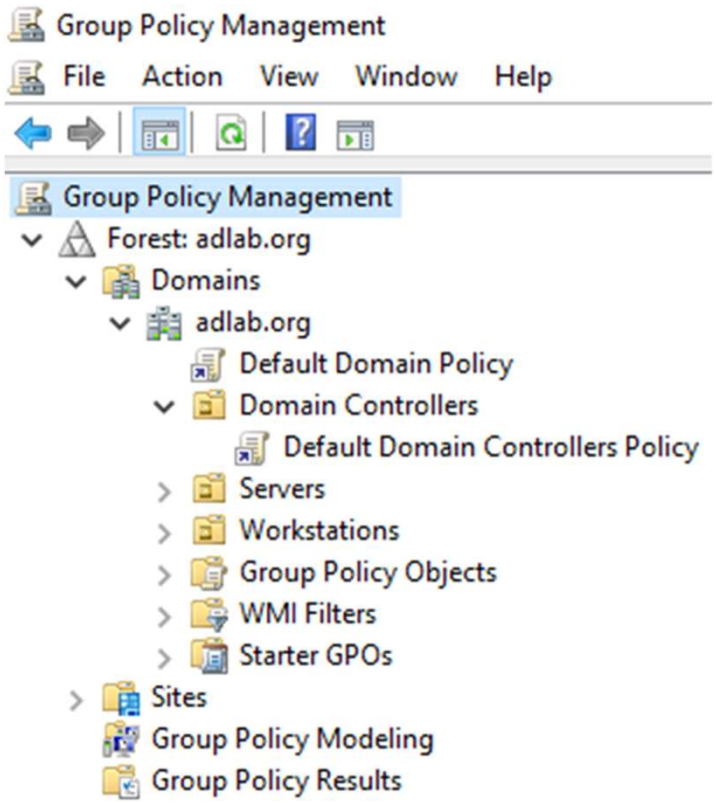
- Serves as a container for a collection of settings, scripts, and administrative templates that define and enforce system settings, security policies, and user/computer configurations
- Applied to specific containers, including sites, domains, or OUs.
- Apply GPOs to specific users, groups, or computers using security filtering
- User and Computer Configuration
- Provides fine-grained control over policy precedence.



BLACK HILLS | Information Security

Group Policy MMC

- Centrally Managed Firewalls
- SIEM
- Centrally Managed Anti-Virus
- EDR
- Application Allow Listing
- Remote Access



Authentication Protocols

NTLM

- older protocol for Windows networks
- Uses a challenge-response mechanism to verify user credentials

Kerberos

- Default protocol in Active Directory
- Uses ticket-granting tickets (TGTs) for secure communication

NTLMv1 and NTLMv2

What is Kerberos?

- The main authentication protocol in Active Directory.
- Inspired by the Greek mythology
- KDC involves three aspects
- Authentication Server (AS)
- Ticket-granting server (TGS)
- Database

PAC

- Contains information about the user's security group memberships, privileges, and other security-related attributes
- Digitally signed by the Key Distribution Center (KDC)
- Used by Domain Controllers and other resources to make access control decisions
- The PAC is included in a users ST

Service Principal Name

- An SPN is how a Kerberos client identifies a service on a system

  Example: MSSQLSvc/db.example.com:1433

- Created and queried with the setspn.exe

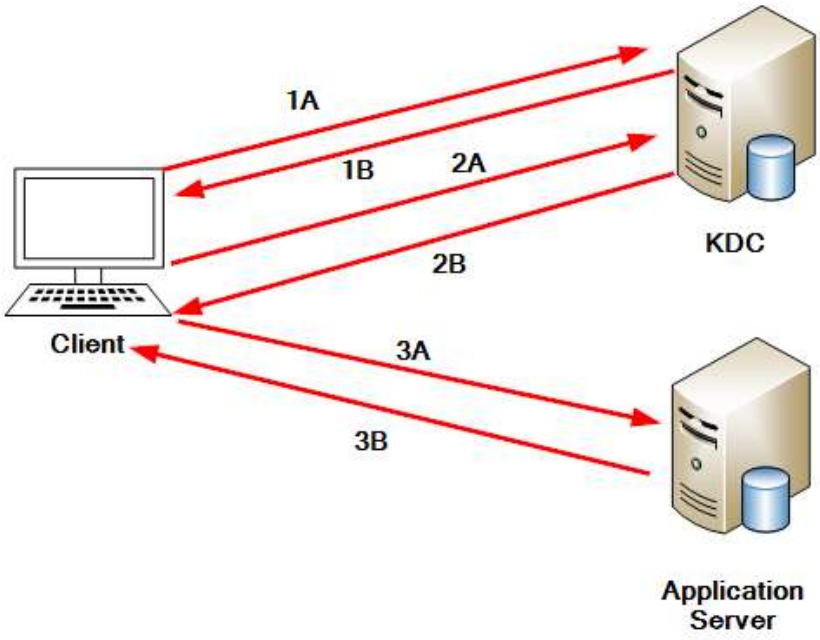
- Each SPN must be unique within the Kerberos realm and must be registered in the (KDC) for the realm where the service is hosted

Kerberos In Action

- 1A. AS REQ (request TGT)
- 1B. AS REP (receive TGT)

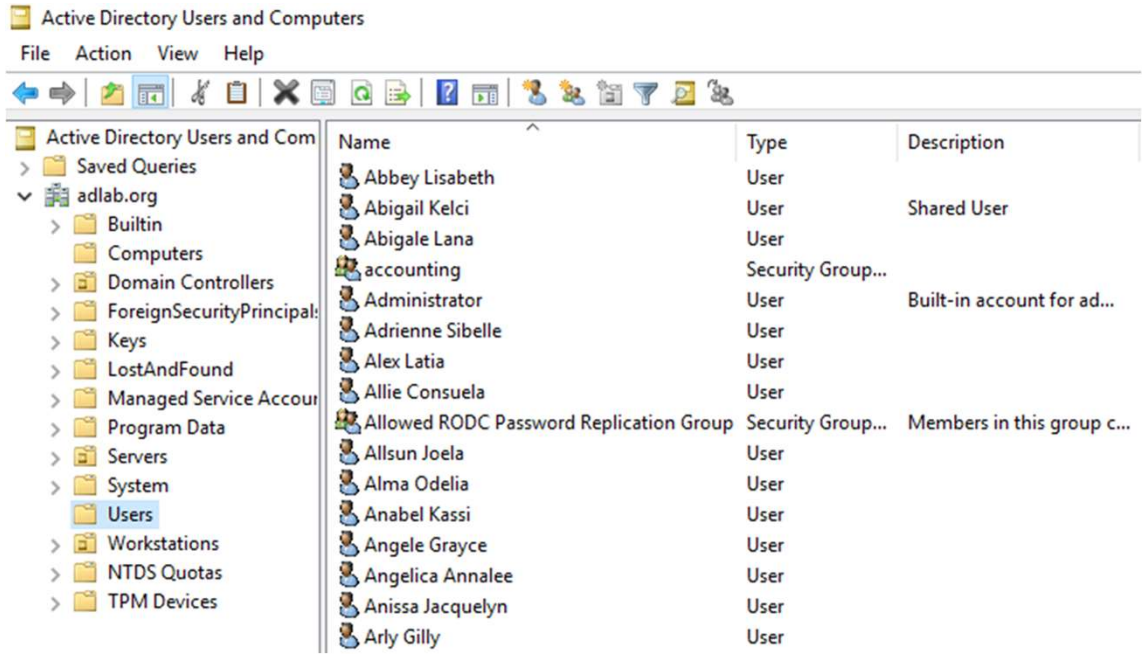
- 2A. TGS REQ (present TGT, Request TGS)
- 2B. TGS REP (receive TGS)

- 3A. Service REQ (present TGS)
- 3B. Service REP (grant access)



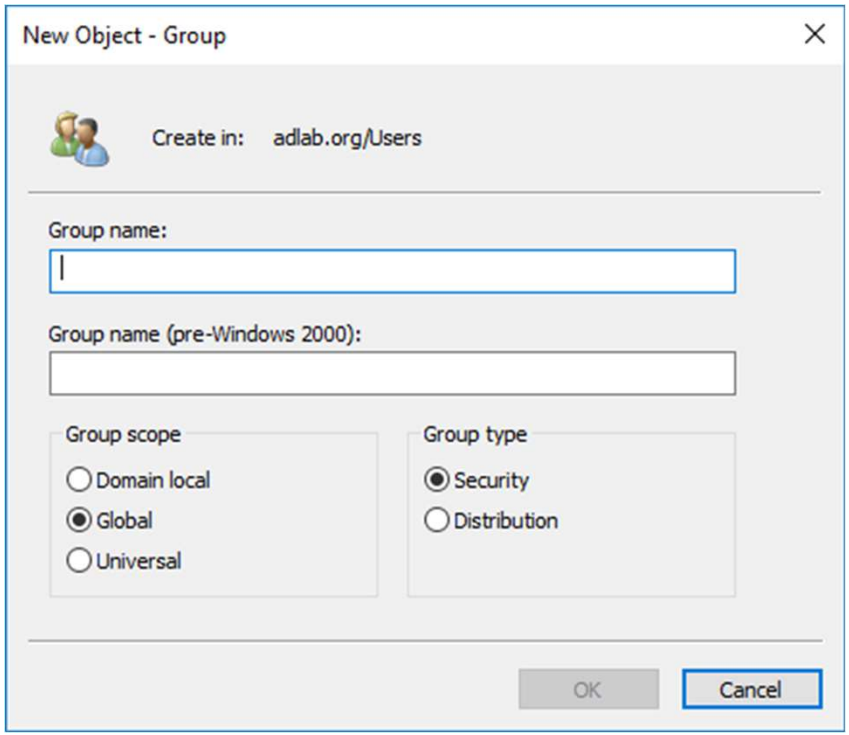
Users and Computers

- Local Users
- Domain Users
- Local Computers
- Domain Computers



BLACK HILLS | Information Security

Groups



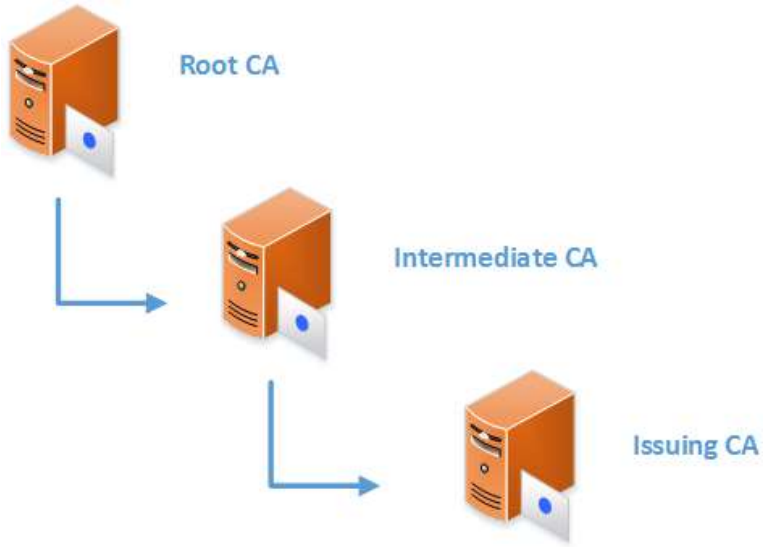
- Domain Local Groups
- Global Groups
- Universal Groups
- Security Groups
- Distribution Groups
- Built-in Groups
- Nested Groups

A D C S

- ADCS (Active Directory Certificate Services) is a Windows server role.
- Provides the infrastructure needed for the management of digital certificates.
- These certificates are used for various purposes, including secure email, web server authentication, user authentication, and secure network communications.
- Supports certificate revocation mechanisms

BLACK HILLS | Information Security

ADCS Components



- Comprehensive public key infrastructure (PKI) solution in the Windows environment

- Certificate Authorities (CAs): Root CA vs. Subordinate CA
- Certificate Templates
- Certificate Revocation Lists (CRLs)
- Certificate Store
- Certificate Clients

Certificate Templates

- Certificate templates are predefined configurations.
- User Certificates
- Computer Certificates
- Web Server Certificates
- Code Signing Certificates
- Smart Card Logon Certificates

BLACK HILLS | Information Security

General Best Practices

- Backup Strategies
- Patch Management
- Change Control
- Monitoring and Auditing
- Security Policies
- Tracking User Activity and Access
- Audit Policies

- https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations

Troubleshooting Tools and Techniques

- Event Viewer
- dcdiag
- netdiag
- repadmin

Performance Optimization

- Optimize DNS Configuration
- Proper Site and Subnet Configuration
- Manage Replication
- Database Maintenance
- Optimize Group Policy Processing
- Monitor and Tune Performance

High Availability and DR

- Redundant Domain Controllers
- Disaster Recovery Plan
- Use Read-Only Domain Controllers (RODCs)
- Implement Fault Tolerance

Security Best Practices

- Implement Least Privilege Principle
- Secure Domain Controllers
- Use Strong Password Policies
- Regularly Audit and Monitor AD
- Implement Group Policy Best Practices
- Protect Against Pass-the-Hash Attacks

BLACK HILLS | Information Security

Disable Insecure Network Protocols

- Disable LLMNR can be performed via group policy
  - Computer Configuration ↠ Administrative Templates ↠ Network ↠ DNS Client ↠ “Turn OFF Multicast Name Resolution”
- Disable NetBIOS over TCP/IP (NBT-NS) (No Native GPO Setting)
  - must be completed manually for each system, OR through either a script or registry setting implemented via Group Policy
  - Network Connections ↠ Network Adapter Properties ↠ Internet Protocol Version 4 (TCP/IPv4) ↠ Advanced settings ↠ WINS tab ↠ “Disable NetBIOS over TCP/IP”
- Implement Network Access Control
- Network Segmentation

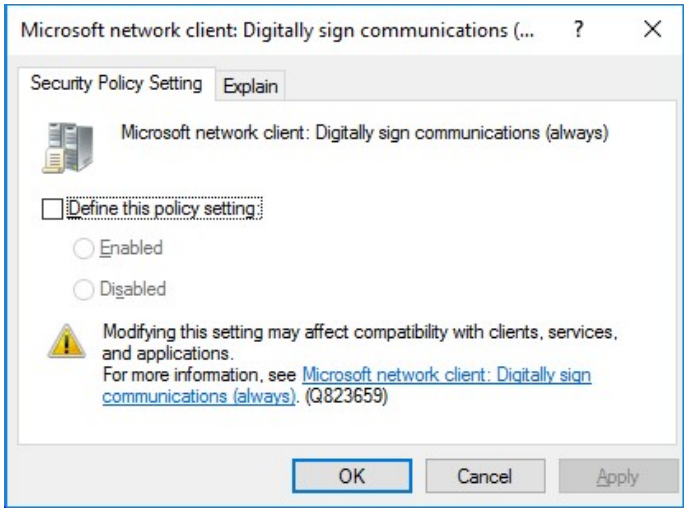
BLACK HILLS | Information Security

SMB Hardening

- Enable SMB Signing.

  "Microsoft network server: Digitally sign communications (always)“

- Disable NTLM authentication and switch to Kerberos
- Utilize Tiered Accounts
- Local Administrator Restrictions
- Protected Users Security Group



https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group

Kerberos Hardening

- Log Analysis
  - Audit Kerberos Authentication Service (GPO)
  - Event IDs 4768, 4769, 4771 and 4770
- Implement Account Lockout Policies and Decoy Accounts
- Service Accounts should have long (30+ characters) passwords and should be changed regularly
- Utilize “Group Managed Service Accounts” (GMSA)
- Implement Windows Defender Credential Guard
- Limit administrative privileges to users
  - Minimize local admin privileges
  - Limit Domain Admins to only log on to Domain Controllers
- Configure time-based restrictions on TGTs and Service Tickets
- Change the KRBTGT password regularly
- Minimize the number of accounts that can access the KRBTGT password hash.

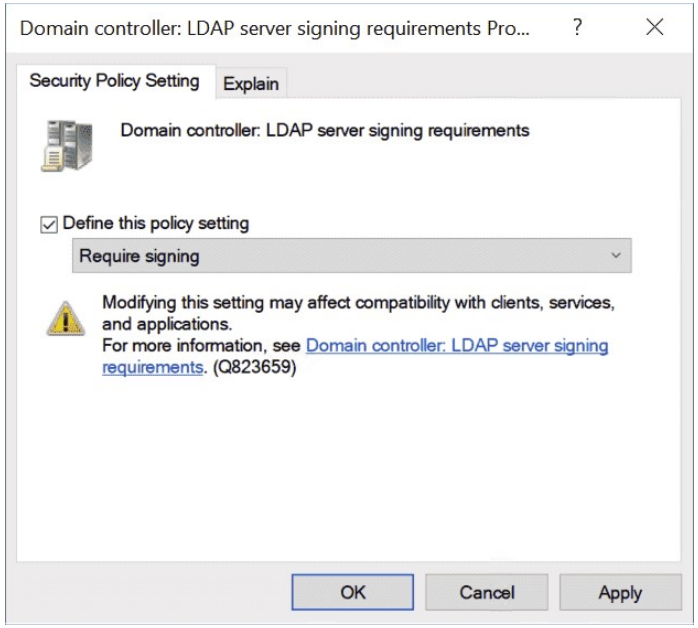
Passwords

- Strong Password Policies
- Minimum passphrase length should be 15 characters
  Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy
- Disable insecure password storage mechanisms
- Multi-Factor Authentication (MFA)
- Use unique passwords for every account
- Audit Logging and Password audits
- Domain Password Audit Tool (DPAT)
  https://github.com/clr2of8/DPAT

Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

IPv6 Hardening

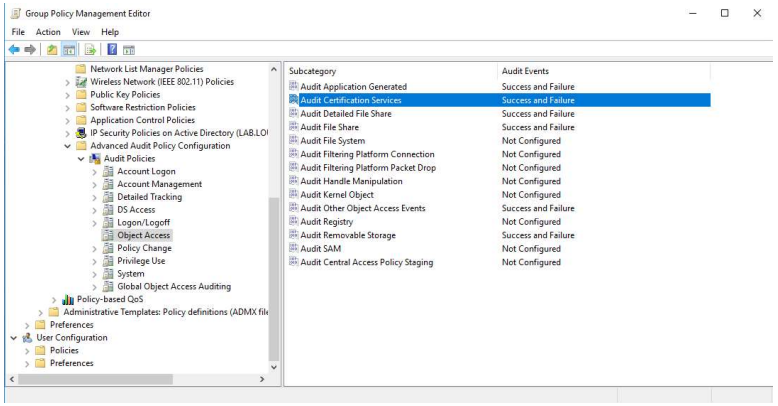
- Disable IPv6
- Windows Firewall Block rules
  - (Inbound) Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-In)
  - (Inbound) Core Networking - Router Advertisement (ICMPv6-In)
  - (Outbound) Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-Out)
- Disable the Proxy Auto detection via Group Policy.
- Disable NTLM entirely and switch to Kerberos



BLACK HILLS | Information Security

ADCS Hardening

- Detections should be built around unexpected template configuration changes
- Enable all CA audit logs
  Event ID's 4768, 4886, 48876, 4899, 4900
- Enable Success/Failure logging of all the Windows advanced audit logs (GPO)
- Enable Success/Failure logging of all the Windows audit logs (GPO)
- Treat CAs as Tier 0 Assets
- Harden CA Settings
- Audit Published Templates
- Harden Certificate Template Settings
- Harden AD CS HTTP Endpoints



- Ceritified Pre-owned Whitepaper
  https://specterops.io/wp-content/uploads/sites/3/2022/06/Certified_Pre-Owned.pdf?ref=labs.lares.comm

BLACK HILLS | Information Security

Takeaways

- Plan Your AD Structure
- Understand the Various Roles
- OU's and GPO's
- User and Group Management
- Authentication Mechanisms
- Security Best Practices

BLACK HILLS | Information Security

Questions?

BLACK HILLS | Information Security