Step C: Active Directory Job Tasks by Experience Level for TrustCare Health Systems

This section outlines Active Directory tasks according to job experience levels, from junior to senior, that you should master in your lab environment. These align with common requirements found in job postings and represent the progression of skills expected in IAM roles.

Junior AD Administrator Tasks (0-2 years experience)

1. User Account Management

- Create, modify, and disable user accounts following company naming conventions
- Perform password resets and account unlocks
- Move user accounts between organizational units
- Update user account properties (contact info, department, manager)
- Execute bulk user creation using templates and CSV imports

Practice Scenario: HR sends an urgent request to create 15 new accounts for pharmacy interns starting tomorrow at various locations. Set up the accounts with appropriate naming conventions and temporary passwords.

2. Group Management

- Create and modify security and distribution groups
- Add and remove users from groups
- Nest groups according to established hierarchies
- Document group purposes and membership criteria
- Verify group membership for access audits

Practice Scenario: The Clinical Research department needs a new set of groups for their medication trial system with proper nesting structure: SG-RD-MedTrials (parent), SG-RD-MedTrials-Read, SG-RD-MedTrials-Modify, and SG-RD-MedTrials-Admin.

3. Basic GPO Management

- Link existing GPOs to OUs
- Modify simple GPO settings under supervision
- Run GPO modeling reports

- Verify GPO application using tools like gpresult
- Document GPO changes in the change management system

Practice Scenario: Link the "ALL-SEC-ScreenTimeout" GPO to all pharmacy workstation OUs and verify it applies correctly to sample computers.

4. Computer Account Management

- Create and reset computer accounts
- Move computer accounts between OUs
- Troubleshoot basic computer account issues
- Join computers to the domain
- Document computer information in the CMDB

Practice Scenario: Prepare for deployment of 20 new pharmacy workstations by pre-creating computer accounts in the CHI-PHARM-Computers OU with proper naming convention.

5. Basic AD Troubleshooting

- Check and verify AD replication status
- Use basic PowerShell commands for AD management
- Monitor for account lockouts and authentication failures
- Perform basic health checks on domain controllers
- Document and escalate complex issues

Practice Scenario: Several users report slow logon times at the Dallas office. Investigate basic metrics on DAL-DC-01 and DAL-DC-02 to identify potential issues.

Mid-level AD Administrator Tasks (2-5 years experience)

6. OU Structure Design and Implementation

- Create and modify OUs based on business requirements
- Implement delegation of control for OUs
- Manage OU permissions and Group Policy inheritance
- Design departmental OU structures
- Document OU design decisions

Practice Scenario: Design and implement a new OU structure for TrustCare's specialty pharmacy business unit that maintains security separation while allowing appropriate delegation.

7. Group Policy Creation and Troubleshooting

- Create and modify complex GPOs
- Troubleshoot GPO application issues
- Implement loopback processing for special cases
- Create and manage WMI filters
- Perform Group Policy results analysis

Practice Scenario: Create a new GPO that implements USB restrictions for workstations handling patient data, but exempts specific devices using WMI filtering and security group filters.

8. PowerShell Automation

- Develop PowerShell scripts for routine AD management tasks
- Create scheduled tasks for regular AD maintenance
- Implement error handling and logging in scripts
- Generate automated reports for compliance
- Document and maintain script repositories

Practice Scenario: Create a PowerShell script that generates daily reports of all inactive user accounts, disabled accounts, and accounts with password expiration in the next 7 days.

9. Advanced User Provisioning

- Implement role-based access control using AD groups
- Manage complex access requirements across systems
- Configure user account templates
- Implement workflow approval processes
- Audit user permissions against job roles

Practice Scenario: Implement the onboarding process for clinical pharmacists who need access to 12 different systems, each with specific permission requirements based on location and specialty.

10. Site and Replication Management

- Configure AD sites and services
- Manage site links and replication schedules
- Monitor replication health and troubleshoot issues
- Optimize authentication traffic
- Document site topology changes

Practice Scenario: Add the new Denver office to the site topology with appropriate site links to headquarters and the nearest regional offices, then verify replication is working properly.

Senior AD Administrator/Engineer Tasks (5+ years experience)

11. Forest and Domain Design

- Design multi-domain forests for large organizations
- Plan for domain consolidation after acquisitions
- Implement forest and domain trusts
- Configure domain and forest functional levels
- Develop domain naming conventions and DNS strategy

Practice Scenario: Design the AD consolidation plan for TrustCare's acquisition of MediPharm Inc., including trust configuration, user migration strategy, and eventual domain consolidation.

12. Advanced Security Hardening

- Implement Privileged Access Management
- Configure time-based, just-in-time administrative access
- Implement Advanced Threat Analytics
- Secure LDAP communications with certificates
- Perform security audits and penetration testing

Practice Scenario: Implement a comprehensive privileged access solution for domain administrators that includes just-in-time elevation, dedicated admin workstations, and enhanced auditing.

13. Disaster Recovery Planning and Testing

- Design and document AD backup strategies
- Implement automated system state backups
- Test domain controller recovery procedures
- Develop business continuity procedures
- Create and maintain runbooks for critical failures

Practice Scenario: Develop and test the disaster recovery procedure for the complete failure of the Atlanta data center, including FSMO role transfers and service restoration.

14. Directory Services Integration

- Integrate Active Directory with cloud services (Azure AD)
- Configure federation services for partner access
- Implement hybrid identity solutions
- Design and implement directory synchronization
- Troubleshoot complex identity flow issues

Practice Scenario: Implement AD FS and configure claims-based authentication for TrustCare's partner portal where external pharmacies can verify prescription information.

15. PKI Implementation and Management

- Design and implement enterprise PKI
- Configure certificate auto-enrollment
- Manage certificate lifecycle
- Implement smart card authentication
- Develop certificate security policies

Practice Scenario: Implement a complete PKI infrastructure for TrustCare, including an offline root CA, enterprise issuing CAs, and certificate templates for different purposes including smart card authentication for clinicians.

Director/Architect Level Tasks (8+ years experience)

16. Identity Governance Strategy

- Develop comprehensive identity management strategies
- Create identity lifecycle management frameworks
- Implement attestation and recertification processes
- Develop identity-related policies and standards
- Create identity metrics and reporting frameworks

Practice Scenario: Design and document a comprehensive identity governance framework for TrustCare that meets healthcare compliance requirements while supporting business agility.

17. Zero Trust Architecture Implementation

- Design identity-centric security models
- Implement conditional access policies
- Configure risk-based authentication
- Develop least-privilege access models
- Create security monitoring and alerting frameworks

Practice Scenario: Design and implement the first phase of a zero trust architecture for TrustCare, focusing on securing access to clinical systems and patient data.

18. Enterprise Directory Services Architecture

- Design global directory services for multinational organizations
- Plan for cloud identity transformation
- Develop identity data quality standards

- Create directory services roadmaps
- Lead directory consolidation programs

Practice Scenario: Create a 3-year strategic roadmap for TrustCare's evolution from on-premises AD to a hybrid model with eventual cloud-first approach for new applications.

19. Compliance Framework Implementation

- Design and implement regulatory compliance controls
- Create automated compliance reporting
- Develop audit frameworks for identity systems
- Implement segregation of duties controls
- Design continuous compliance monitoring

Practice Scenario: Develop and implement a comprehensive compliance framework for TrustCare's Active Directory that meets HIPAA, HITECH, and PCI-DSS requirements with automated reporting.

20. Identity-as-a-Service Design

- Architect modern identity service offerings
- Implement identity API frameworks
- Design self-service identity platforms
- Create identity orchestration workflows
- Develop identity data integrity models

Practice Scenario: Design an internal Identity-as-a-Service platform for TrustCare that will provide unified identity services to all business units and applications through standardized APIs.

Additional Healthcare-Specific AD Tasks

21. HIPAA-Compliant Audit Implementation

- Configure detailed audit logging for PHI access
- Implement separation of duties for pharmacists and technicians
- Create healthcare-specific reports for compliance audits
- Configure alerts for suspicious access patterns
- Document compliance controls for regulatory inspections

Practice Scenario: Configure and test a comprehensive audit solution that tracks all access to patient prescription records within the pharmacy system.

22. Electronic Prescribing Security

- Implement two-factor authentication for e-prescribing credentials
- Configure secure certificate management for DEA compliance
- Create role separation for controlled substance prescribing
- Implement specialized security groups for prescriber access
- Document controls for DEA and state pharmacy board compliance

Practice Scenario: Configure the authentication and authorization framework for TrustCare's new electronic prescribing system for controlled substances, meeting all DEA requirements.

23. Clinical System Integration

- Configure service accounts for Epic EHR integration
- Implement specialized security groups for clinical roles
- Create login scripts for clinical workstations
- Configure Fast User Switching for shared clinical workstations
- Implement location-aware access controls for clinical systems

Practice Scenario: Configure and test the AD integration with TrustCare's new clinical laboratory system, including proper service accounts, security groups, and access controls.

These tasks represent a comprehensive progression of Active Directory skills across different experience levels in a healthcare organization. By systematically working through these scenarios in your lab environment, you'll develop a robust skill set that directly maps to employer requirements and real-world challenges in healthcare IAM.

Each task builds upon previous ones, and mastering them will demonstrate your capability to handle increasingly complex directory services responsibilities. This structured approach ensures your lab experience will translate directly to marketable skills for your career advancement.