Step B: Comprehensive List of Daily Administrative Tasks for TrustCare Health Systems Active Directory

As an IAM Architect/Engineer for TrustCare Health Systems, you'll need to perform various administrative tasks to maintain the Active Directory infrastructure. Below are 20 realistic scenarios you can practice in your lab environment, ranging from routine to complex tasks.

User Account Management Scenarios

1. New Employee Onboarding

Scenario: HR has provided a list of 5 new pharmacy technicians starting next Monday at the Chicago location. Create their user accounts following TrustCare's naming convention, place them in the appropriate OU structure, and assign group memberships for essential pharmacy applications.

Requirements:

- Create accounts: cmorales, lbaker, tpham, jwilson, and rnguyen
- Place in CHI-PHARM-Users OU
- Add to groups: SG-PHARM-R-RxManagerPro, SG-PHARM-RW-InventorySystem, SG-ALL-OfficeApps, DL-Pharmacy-Staff

2. Employee Department Transfer

Scenario: Jessica Garcia (jgarcia) is transferring from Customer Support to the HR department at headquarters. Update her account attributes, move to the appropriate OU, and modify group memberships accordingly.

Requirements:

- Move from OU=SUPP,OU=Users,OU=HQ,DC=trustcare,DC=corp to OU=HR,OU=Users,OU=HQ,DC=trustcare,DC=corp
- Update department attribute from "Customer Support" to "Human Resources"
- Remove from SG-SUPP-RW-TicketSystem
- Add to SG-HR-RW-HRISSystem and SG-HR-R-PersonnelFiles

3. Executive Account Configuration

Scenario: The new Chief Medical Officer, Dr. Robert Chang (r.chang), requires a high-security account with specific permissions. Create his account with appropriate settings and group memberships.

Requirements:

- Create in OU=EXEC,OU=Users,OU=HQ,DC=trustcare,DC=corp
- Set password never expires
- Enable smart card requirement
- Add to groups: SG-EXEC-ClinicalLeadership, SG-EXEC-StrategicPlanning, SG-ALL-TeleHealthAdmins
- Configure access to restricted clinical data through appropriate security groups

4. Multiple Account Termination

Scenario: Five employees have left the company. Disable their accounts, move them to the terminated users OU, and document the process for audit purposes.

Requirements:

- Disable accounts: mbrown, sjohnson, tsmith, rlee, and dnguyen
- Move to OU=Terminated,OU=Users,DC=trustcare,DC=corp
- Remove from all security groups
- Document the actions taken for compliance records
- Set account expiration date for 90 days in the future (for audit purposes)

5. Password Reset with Secure Notification

Scenario: Three users from the Finance department have submitted urgent password reset requests through the helpdesk system. Reset their passwords following the company's secure notification protocol.

Requirements:

- Reset passwords for kthomas, jchang, and rwilliams
- Follow secure password distribution process
- Document the reset in the ticketing system
- Ensure users change passwords at next logon

Group and Permission Management Scenarios

6. Create Nested Security Groups for Pharmacy Department

Scenario: Design and implement a nested group structure for the new specialty pharmacy department to provide granular access control to oncology medication systems.

Requirements:

- Create parent group SG-PHARM-SpecialtyOncology
- Create child groups for different access levels (Read, ReadWrite, Admin)
- Nest appropriate groups
- Document the group hierarchy
- Add 10 test users to appropriate groups based on their roles

7. Implement Time-Based Access Restrictions

Scenario: Implement time-based access restrictions for pharmacy technicians who should only have system access during business hours (7 AM to 9 PM local time).

Requirements:

- Identify all accounts in the Pharmacy Technician security group
- Configure logon hour restrictions
- Implement exceptions for designated on-call staff
- Create a GPO to enforce workstation logoff after hours

8. Delegated Administration for Regional IT Support

Scenario: Configure delegated permissions for regional IT support teams to manage user accounts and group memberships within their geographic locations only.

Requirements:

- Create SG-IT-RegionalAdmins-[Location] groups for each regional office
- Configure delegation settings to allow password resets, group membership changes, and computer management
- Restrict delegation to specific OUs based on location
- Document the delegation model for security review

9. Role-Based Access Control Implementation

Scenario: Implement a role-based access control model for the new telehealth platform, creating security groups based on clinical roles rather than departments.

Requirements:

- Create groups for different clinical roles (Physicians, Nurses, Technicians, Support)
- Define access levels for each role
- Map existing users to appropriate role-based groups
- Test access to ensure proper permissions

10. Group Policy Delegation

Scenario: Delegate GPO management permissions to the IT security team for security-related policies only, while restricting their ability to modify application deployment policies.

Requirements:

- Create a security group for policy administrators
- Configure delegation settings in Group Policy Management
- Set granular permissions for specific GPO categories
- Document the delegation model

Computer and System Management Scenarios

11. Deploy Domain Controllers for New Location

Scenario: TrustCare is opening a new regional office in Denver. Plan and implement new domain controllers to support this location following the company's DC naming standards.

Requirements:

- Create two new DCs (DEN-DC-01, DEN-DC-02)
- Configure site and replication settings
- Implement proper DNS and DHCP settings
- Verify replication is working correctly
- Document the new site topology

12. Mass Computer Migration for Department Reorganization

Scenario: The Miami office is reorganizing, and 50 computer accounts need to be moved to different OUs based on new department assignments. Create and execute a script to handle this migration efficiently.

Requirements:

- Identify computers in current OUs
- Create a CSV mapping file with computer names and target OUs
- Write and test a PowerShell script to perform the migration
- Verify all computer accounts are in their correct OUs
- Document the migration process

13. Secure Service Account Creation

Scenario: Create service accounts for the new medication dispensing system that requires special permissions but must follow security best practices.

Requirements:

- Create service accounts with appropriate naming convention (SVC-MedDispense-[Service])
- Configure managed service accounts where appropriate
- Set secure password policies
- Document account purpose and access levels
- Implement least privilege principle

14. Group Policy Implementation for HIPAA Compliance

Scenario: Implement and test new Group Policy Objects to ensure workstations comply with HIPAA security requirements.

Requirements:

- Create GPOs for screen lock timeouts (2 minutes for clinical systems)
- Configure USB device restrictions
- Implement BitLocker requirements
- Set up advanced audit policies
- Test and document the impact on sample workstations

15. Domain Controller Health Check Automation

Scenario: Create and implement an automated health checking process for all domain controllers across the organization.

Requirements:

- Write PowerShell scripts to check DC health metrics
- Configure scheduled tasks to run health checks daily
- Create a reporting mechanism for issues
- Test the solution by simulating common DC issues
- Document remediation procedures

Advanced Administration Scenarios

16. Active Directory Certificate Services Deployment

Scenario: Deploy a two-tier PKI infrastructure to support smart card authentication for clinicians and secure email communication.

Requirements:

- Set up offline root CA

- Configure enterprise subordinate CA
- Create certificate templates for different purposes
- Configure auto-enrollment policies
- Document the certificate lifecycle management process

17. Implement Privileged Access Management

Scenario: Implement just-in-time administrative access for Domain Admins and other privileged accounts to enhance security.

Requirements:

- Create tiered admin accounts (Tier 0, 1, 2)
- Configure time-limited group membership
- Implement administrative workstation restrictions
- Set up enhanced monitoring for privileged activities
- Document the privileged access workflow

18. Multi-Factor Authentication for Remote Access

Scenario: Configure multi-factor authentication for all remote access to TrustCare's network, particularly for clinicians accessing patient records remotely.

Requirements:

- Configure NPS with RADIUS for VPN authentication
- Set up certificate-based authentication
- Create security groups for MFA exemptions (special cases only)
- Test various authentication scenarios
- Document the configuration for compliance purposes

19. Active Directory Site Topology Optimization

Scenario: Review and optimize the site topology and replication for TrustCare's expanding network to minimize authentication latency and WAN traffic.

Requirements:

- Review current site links and costs
- Analyze replication traffic patterns
- Reconfigure site links based on network bandwidth
- Optimize replication schedules
- Document the new topology with justifications

20. Active Directory Federation Setup for Partner Access

Scenario: Implement AD FS to allow secure partner access to TrustCare's prescription verification portal without requiring partner users to have TrustCare accounts.

Requirements:

- Install and configure AD FS servers
- Configure claims rules for partners
- Set up relying party trusts
- Implement appropriate access controls
- Test federation with a sample partner organization
- Document the federation architecture and security controls

These 20 scenarios cover a wide range of Active Directory administrative tasks relevant to healthcare environments like TrustCare Health Systems. By practicing these scenarios in your lab environment, you'll gain valuable hands-on experience with both routine and complex IAM tasks that are directly applicable to real-world healthcare organizations. Each scenario presents unique challenges related to security, compliance, and operational efficiency that you would face as an IAM professional in this industry.