 

This is a Job Posting for Junior IAM positions. For the last week I have been able to build my foundation on IAM using the TrustCare project. Look At the job responsibilities for Xtensys. Using the TrustCare scenario, create me a project task that meets all the job responsibilities. You can make up 5 or more tasks to perform for each responsibility. In a separate study I want to take these and run a lab scenario this weekend and gain real work experience applicable to this job. Make as many tasks as possible. Don't stop at Junior, create Mid and Senior tasks as extra challenges. Be rigorous

# Project Tasks for Junior IAM Role Based on TrustCare Scenario

I'll create a comprehensive set of project tasks based on the Xtensys job responsibilities, using the TrustCare Health Systems scenario as a foundation. These tasks will provide you with practical experience that directly aligns with the requirements of the Junior IAM position.

## Core Task Categories

### 1. Directory Services Management

#### Junior Level Tasks
1. **User Account Lifecycle Management**
   - Create 10 new standard user accounts for pharmacy technicians following TrustCare's naming convention
   - Disable 5 terminated employee accounts and move them to the Terminated Users OU
   - Update department attributes for 8 users who transferred from Customer Support to HR
   - Reset passwords for 3 finance department users who are locked out
   - Document the user provisioning process for audit purposes

2. **Group Management**
   - Create a nested security group structure for the Specialty Pharmacy department
   - Audit membership of sensitive groups like SG-PHARM-RW-ControlledSubstances
   - Add 5 new physicians to the appropriate clinical role groups
   - Remove access for terminated employees from all security groups
   - Document the group hierarchy and access permissions

3. **OU Structure Administration**
   - Move computer accounts for the Miami office into their correct department OUs
   - Create a new OU for the Denver regional office
   - Implement delegation of control for regional IT support staff
   - Update OU descriptions for documentation purposes
   - Verify that all objects are in their appropriate OUs

4. **Computer Account Management**
   - Create 15 computer accounts for new pharmacy workstations
   - Move workstation accounts for the reorganized Miami office

 

- Reset computer accounts for reimaged devices
- Document naming standards for all computer accounts
- Verify computer account placement in appropriate OUs

#### Mid-Level Tasks
1. **Advanced Permission Management**
   - Implement role-based access control for the e-prescribing system
   - Configure Just Enough Administration (JEA) for helpdesk technicians
   - Implement time-based access restrictions for pharmacy technicians (7AM-9PM)
   - Audit and remediate excessive permissions on sensitive OUs
   - Document permission changes in the change management system

2. **Site and Replication Management**
   - Configure AD sites and services for the new Denver office
   - Optimize site links between regional offices
   - Monitor replication health across all domain controllers
   - Troubleshoot replication issues between Atlanta and Dallas
   - Document the site topology and replication schedule

### 2. Identity Access Management (IAM) Platform Administration

#### Junior Level Tasks
1. **MFA Implementation**
   - Configure Duo MFA for 10 pilot users in the IT department
   - Document the MFA enrollment process for end users
   - Test MFA functionality for remote access scenarios
   - Create troubleshooting guides for common MFA issues
   - Generate reports on MFA adoption rates

2. **Beyond Trust Administration**
   - Create vendor accounts in the vendor portal
   - Configure session timeouts for vendor access
   - Audit vendor activities in the portal
   - Update access levels for existing vendors
   - Document the vendor onboarding process

3. **Access Policy Implementation**
   - Apply password policies to user accounts
   - Configure account lockout thresholds
   - Implement password complexity requirements
   - Document policy exceptions for service accounts
   - Create reports on policy compliance

#### Mid-Level Tasks

 

1. **Advanced IAM Configuration**
   - Implement Azure AD Connect sync for hybrid identity
   - Configure conditional access policies based on device compliance
   - Set up risk-based authentication for sensitive applications
   - Integrate IAM with clinical applications using SAML
   - Document the complete identity lifecycle management process

2. **Certificate Management**
   - Deploy certificates for smart card authentication
   - Configure auto-enrollment policies
   - Implement certificate lifecycle management
   - Document certificate issuance and revocation procedures
   - Audit certificate usage for compliance purposes

### 3. First-Level Support

#### Junior Level Tasks
1. **Account Troubleshooting**
   - Resolve login issues for 5 users unable to access the RxManager application
   - Troubleshoot account lockouts for finance department staff
   - Fix group membership issues preventing access to shared resources
   - Document resolution steps in the ticketing system
   - Create a knowledge base article for common account issues

2. **Password Management**
   - Process 10 password reset requests following secure notification protocols
   - Verify user identity before processing resets
   - Document all password reset activities for compliance
   - Configure self-service password reset for pilot users
   - Create user guides for password reset procedures

3. **Access Resolution**
   - Troubleshoot access issues for new hires unable to access email
   - Resolve permission problems for clinical staff accessing patient records
   - Fix login issues for pharmacy workstations
   - Document all access-related tickets for compliance reporting
   - Create training materials for common access problems

#### Mid-Level Tasks
1. **Complex Access Troubleshooting**
   - Resolve cross-domain authentication issues for recently acquired companies
   - Troubleshoot certificate-based authentication problems
   - Fix delegation issues for departmental administrators
   - Create diagnostic scripts for common access problems

 

- Document complex issue resolution for knowledge sharing

### 4. Security Policy Enforcement

#### Junior Level Tasks
1. **Policy Monitoring**
   - Run reports to identify accounts not complying with password policies
   - Monitor for disabled security settings on workstations
   - Verify MFA enforcement for remote access
   - Document compliance exceptions with appropriate approvals
   - Generate weekly policy compliance reports

2. **Security Group Maintenance**
   - Audit membership of privileged security groups
   - Remove unnecessary access rights based on least privilege principle
   - Update security group memberships based on job role changes
   - Document all changes to security-related groups
   - Generate quarterly access review reports

3. **Security Control Implementation**
   - Apply GPOs for USB device restrictions on clinical workstations
   - Configure screen timeout policies for shared workstations
   - Implement BitLocker encryption policies
   - Document security control configurations
   - Verify policy application on sample systems

#### Mid-Level Tasks
1. **Advanced Security Configuration**
   - Implement Credential Guard on administrative workstations
   - Configure Protected Users security group for privileged accounts
   - Set up Advanced Audit Policy Configuration
   - Deploy LAPS (Local Administrator Password Solution)
   - Document security hardening procedures

2. **Security Assessment**
   - Conduct security assessment using PingCastle
   - Address top 10 security findings
   - Implement secure LDAP (LDAPS) for all directory communications
   - Document remediation steps for security issues
   - Create security compliance reports for auditors

### 5. System Monitoring

#### Junior Level Tasks

 

1. **Directory Service Monitoring**
   - Monitor domain controller performance metrics
   - Check replication status between sites
   - Verify FSMO role availability
   - Document monitoring procedures
   - Create daily health check reports

2. **Security Monitoring**
   - Monitor for suspicious login attempts
   - Track privileged group membership changes
   - Alert on unauthorized access attempts
   - Document security incidents
   - Generate weekly security reports

3. **Performance Monitoring**
   - Track LDAP query performance
   - Monitor authentication response times
   - Check for resource constraints on domain controllers
   - Document performance baselines
   - Create performance trend reports

#### Mid-Level Tasks
1. **Advanced Monitoring Implementation**
   - Deploy Microsoft Advanced Threat Analytics
   - Configure behavior analytics baselines
   - Set up alerts for Kerberoasting and Pass-the-Hash activities
   - Integrate with SIEM solution
   - Document incident response procedures for detected threats

### 6. System Audits and Reporting

#### Junior Level Tasks
1. **Compliance Reporting**
   - Generate user access reports for quarterly reviews
   - Create reports of inactive accounts
   - Document account lockout events
   - Produce MFA compliance reports
   - Generate password policy compliance reports

2. **Security Auditing**
   - Configure detailed object access auditing for sensitive AD containers
   - Generate reports of privileged account usage
   - Document changes to security-related GPOs
   - Create audit trails for compliance purposes

 

- Verify audit policy implementation

3. **Change Documentation**
   - Document all changes to AD structure
   - Record security group modifications
   - Log policy updates
   - Create change management records
   - Maintain documentation for audit purposes

#### Mid-Level Tasks
1. **Advanced Audit Configuration**
   - Implement comprehensive auditing for HIPAA compliance
   - Configure audit collection for centralized logging
   - Set up automated compliance reporting
   - Create custom audit policies for sensitive operations
   - Document audit framework for regulatory review

### 7. Identity Governance Initiatives

#### Junior Level Tasks
1. **Access Reviews**
   - Assist with quarterly access reviews for clinical departments
   - Generate access reports for managers to review
   - Update group memberships based on review results
   - Document completed reviews for compliance
   - Create access review summary reports

2. **Policy Implementation**
   - Apply new password policies across OUs
   - Implement account lockout policies
   - Configure screen timeout policies
   - Document policy implementations
   - Verify policy application

#### Mid-Level Tasks
1. **Governance Framework Implementation**
   - Implement attestation processes for access rights
   - Configure automated access certification workflows
   - Develop role-based access control models
   - Create separation of duties controls
   - Document governance procedures for compliance

### 8. Scripting and Automation

 

#### Junior Level Tasks
1. **Basic PowerShell Scripts**
   - Create a script to generate inactive user reports
   - Develop a script for bulk user creation from CSV
   - Write a script to check password expiration and notify users
   - Document all scripts with clear comments
   - Maintain a script repository with version control

2. **Scheduled Tasks**
   - Set up automated group membership reports
   - Configure scheduled tasks for inactive account identification
   - Create automated notification for expiring passwords
   - Document scheduled task configurations
   - Monitor execution of automated tasks

#### Mid-Level Tasks
1. **Advanced Automation**
   - Develop comprehensive user provisioning/deprovisioning scripts
   - Create advanced reporting dashboards with PowerShell
   - Build automation for compliance reporting
   - Implement error handling and logging in all scripts
   - Document complete automation framework

## Senior Level Challenges

### 1. Enterprise Architecture Design
   - Design a comprehensive identity governance framework for TrustCare
   - Develop a zero-trust architecture plan for healthcare identity security
   - Create a roadmap for cloud identity transformation
   - Design a privileged access management solution
   - Develop a complete IAM security architecture document

### 2. Advanced Security Implementation
   - Implement a comprehensive privileged access security model
   - Deploy a complete PKI infrastructure with smart card authentication
   - Configure a secure bastion host environment for administrative access
   - Implement advanced threat protection for directory services
   - Design and deploy a comprehensive security monitoring solution

### 3. Identity Integration Architecture
   - Design federation services for partner healthcare organizations
   - Implement claims-based authentication for the e-prescribing portal
   - Develop a hybrid identity strategy with seamless authentication
   - Create an identity API framework for application integration

 

- Design a complete identity-as-a-service offering for internal applications

### 4. Compliance Framework Design
- Develop a comprehensive HIPAA compliance framework for directory services
- Design automated compliance reporting mechanisms
- Create a complete audit strategy for regulatory requirements
- Implement data sovereignty controls for international expansion
- Design a comprehensive identity data lifecycle management strategy

### 5. Disaster Recovery and Business Continuity
- Design a complete AD disaster recovery plan
- Implement automation for forest recovery procedures
- Create business continuity procedures for critical authentication services
- Develop incident response playbooks for directory compromise scenarios
- Design a resilient multi-site authentication architecture

## Implementation Plan

To make the most of your weekend lab scenario:

1. **Start with Junior Tasks**: Begin with core user and group management tasks to establish your foundation
2. **Progress to Mid-Level**: Move to more complex configurations like MFA and security policy implementation
3. **Document Everything**: Create proper documentation for all tasks as you would in a real work environment
4. **Challenge Yourself**: Attempt at least one senior level task to stretch your skills
5. **Create a Portfolio**: Compile your work into a portfolio that demonstrates your capabilities for the interview

This comprehensive set of tasks will provide you with hands-on experience that directly aligns with the requirements in the Xtensys job description, using the TrustCare scenario as your real-world context.