

What if this additional responsibility was mentioned as "Experience with IAM solutions such as Okta, Azure AD, SailPoint, Ping, CyberArk, or ForgeRock." Can you come up with additional tasks and scenarios I could do to meet these requirements? Please keep the same rigor

Additional IAM Platform-Specific Tasks for TrustCare Scenario

I'll create additional rigorous tasks focusing specifically on the IAM solutions mentioned in the job responsibility: "Experience with IAM solutions such as Okta, Azure AD, SailPoint, Ping, CyberArk, or ForgeRock." These tasks will complement your TrustCare lab scenario and provide you with hands-on experience with these enterprise IAM platforms.

Azure AD Tasks

Junior Level Tasks

1. **Azure AD Connect Implementation**
   - Install and configure Azure AD Connect to synchronize TrustCare's on-premises AD with Azure AD
   - Configure password hash synchronization for cloud authentication
   - Set up filtered synchronization to only include specific OUs (e.g., exclude terminated users)
   - Configure attribute filtering to limit synchronized attributes
   - Test and verify synchronization is working properly for new and modified accounts

2. **Basic Azure AD User Management**
   - Create cloud-only user accounts for contractors not in the on-premises directory
   - Assign licenses for Microsoft 365 applications to appropriate users
   - Configure user attribute mapping between on-premises AD and Azure AD
   - Set up dynamic groups based on department attributes (e.g., Pharmacy, Finance)
   - Generate reports on license usage and assignment

3. **Azure MFA Configuration**
   - Enable per-user MFA for administrative accounts
   - Configure MFA registration policies
   - Set up authentication methods (phone, authenticator app)
   - Create testing documentation for end-user MFA experience
   - Generate MFA status reports for compliance purposes

4. **Basic Conditional Access**
   - Create a conditional access policy requiring MFA for all cloud app access
   - Configure location-based conditional access for remote pharmacy access
   - Set up device compliance policies for clinical workstations
   - Test and document conditional access policy outcomes
   - Create end-user guidance for conditional access requirements

Mid-Level Tasks

1. **Advanced Azure AD Integration**
   - Configure Pass-through Authentication with seamless SSO
   - Implement Azure AD Application Proxy for legacy healthcare application access
   - Set up Azure AD B2B collaboration for external healthcare partners
   - Configure Azure AD Connect health monitoring
   - Document the complete hybrid identity architecture

2. **Comprehensive Conditional Access**
   - Implement risk-based conditional access policies
   - Configure context-aware access policies for clinical applications
   - Set up device-based conditional access with Intune integration
   - Create location-based policies for restricted access to PHI
   - Design a zero-trust access model for remote clinical staff

3. **Azure AD Security Configuration**
   - Implement Privileged Identity Management for just-in-time access
   - Configure Identity Protection risk policies
   - Set up access reviews for privileged role assignments
   - Implement Azure AD Password Protection
   - Create a comprehensive security monitoring dashboard

Senior Level Tasks

1. **Enterprise Azure AD Architecture**
   - Design a multi-tenant Azure AD architecture for TrustCare's acquisitions
   - Implement a comprehensive cloud IAM governance framework
   - Design custom RBAC for healthcare-specific scenarios
   - Create an automated provisioning/deprovisioning workflow with Logic Apps
   - Develop a complete cloud identity security architecture document

Okta Tasks

Junior Level Tasks

1. **Okta Basic Implementation**
   - Configure Okta directory integration with TrustCare's Active Directory
   - Set up user provisioning from AD to Okta
   - Create basic user profiles and mapping
   - Configure password policies
   - Test authentication flows for new users

2. **Okta Application Integration**

- Configure SSO for TrustCare's RxManager and MedSync applications
- Set up SAML integration with Epic EHR system
- Configure basic access policies for applications
- Test and document application access flows
- Create user guides for application access

3. **Okta MFA Configuration**
   - Set up Okta Verify for multi-factor authentication
   - Configure SMS and voice call factors as alternatives
   - Create MFA enrollment policies for different user groups
   - Test MFA workflows for clinical and administrative users
   - Document MFA troubleshooting procedures

Mid-Level Tasks

1. **Advanced Okta Integration**
   - Implement Okta's Lifecycle Management for automated provisioning
   - Configure just-in-time provisioning to cloud applications
   - Set up attribute-level mastering between AD and Okta
   - Create custom transformations for healthcare-specific attributes
   - Document the complete identity lifecycle workflow

2. **Okta API Integration**
   - Develop custom scripts using Okta's REST APIs for reporting
   - Create automated user provisioning workflows
   - Implement custom hooks for healthcare workflow integration
   - Build integration with TrustCare's custom pharmacy applications
   - Document API integration architecture

3. **Advanced Authentication Policies**
   - Implement risk-based authentication for clinical access
   - Configure location and network-based access policies
   - Set up step-up authentication for e-prescribing of controlled substances
   - Create device trust policies for clinical workstations
   - Design and document a complete authentication policy framework

Senior Level Tasks

1. **Enterprise Okta Architecture**
   - Design a multi-tenant Okta implementation for TrustCare's expansion
   - Create a comprehensive delegation model for distributed administration
   - Implement a complete governance framework with attestation
   - Design and document disaster recovery procedures
   - Develop custom workflows for healthcare compliance requirements

SailPoint Tasks

Junior Level Tasks

1. **SailPoint IdentityIQ Basics**
   - Configure AD connector for SailPoint IdentityIQ
   - Set up basic identity aggregation
   - Create user attribute correlation rules
   - Generate basic identity reports
   - Document the identity aggregation process

2. **Access Request Management**
   - Configure basic access request workflows
   - Set up approval processes for clinical application access
   - Create access request forms for common healthcare roles
   - Test and document the request process
   - Generate access request reports

3. **Basic Certification Campaigns**
   - Set up quarterly access review campaigns for pharmacy systems
   - Configure manager certification workflows
   - Create certification reports for compliance
   - Document the certification process
   - Generate access review metrics

Mid-Level Tasks

1. **Advanced SailPoint Integration**
   - Configure multiple authoritative sources (HR, AD, clinical systems)
   - Set up complex correlation rules for identity reconciliation
   - Implement role mining and discovery
   - Create automated provisioning workflows for clinical applications
   - Document the complete identity governance architecture

2. **Role-Based Access Control Implementation**
   - Design and implement role models for healthcare staff
   - Create business roles for clinical specialties
   - Configure IT roles for application access
   - Implement role-based provisioning rules
   - Document the complete RBAC framework

3. **Compliance Controls**
   - Implement segregation of duties policies

- Configure policy violation detection and remediation
- Create automated compliance reports for HIPAA requirements
- Set up continuous monitoring of high-risk entitlements
- Document the compliance control framework

Senior Level Tasks

1. **Enterprise SailPoint Architecture**
   - Design a comprehensive identity governance program
   - Implement automated lifecycle state management
   - Create custom integrations with healthcare-specific applications
   - Design a complete attestation framework
   - Develop a governance maturity roadmap with metrics

CyberArk Tasks

Junior Level Tasks

1. **CyberArk Privilege Cloud Setup**
   - Configure AD integration with CyberArk
   - Set up basic privileged account discovery
   - Create basic privileged accounts in the vault
   - Configure password rotation policies
   - Test password retrieval workflows

2. **Basic Session Management**
   - Configure session recording for administrator access
   - Set up basic connection components for Windows servers
   - Create access workflows for domain administrators
   - Test privileged session monitoring
   - Document session management procedures

3. **Application Password Management**
   - Onboard service accounts for pharmacy applications
   - Configure automatic password rotation
   - Set up application-to-application password management
   - Test application authentication with rotated credentials
   - Document application password management procedures

Mid-Level Tasks

1. **Advanced Privileged Access Workflows**
   - Implement just-in-time privileged access
   - Configure dual control workflows for high-risk systems

- Set up privileged session isolation
- Create emergency access procedures
- Document complete PAM workflows

2. **Endpoint Privilege Management**
   - Deploy CyberArk Endpoint Privilege Manager
   - Configure least privilege policies for workstations
   - Implement application control for clinical workstations
   - Set up credential theft protection
   - Document endpoint privilege management architecture

3. **Advanced Monitoring and Auditing**
   - Configure privileged threat analytics
   - Set up real-time monitoring for suspicious activities
   - Create custom reports for compliance
   - Implement integration with SIEM
   - Document the complete monitoring framework

Senior Level Tasks

1. **Enterprise PAM Architecture**
   - Design a comprehensive PAM program for TrustCare
   - Implement segregation of duties controls
   - Create a complete privileged account governance framework
   - Design disaster recovery procedures for privileged access
   - Develop metrics for privileged access risk management

Ping Identity Tasks

Junior Level Tasks

1. **PingFederate Basic Setup**
   - Configure PingFederate server for TrustCare
   - Set up connection to Active Directory
   - Create basic authentication policies
   - Configure password credential validators
   - Test basic authentication flows

2. **Application SSO Integration**
   - Configure SAML connections for healthcare applications
   - Set up OAuth/OIDC for modern applications
   - Create basic SSO policies
   - Test application access workflows
   - Document SSO implementation

3. **PingID MFA Configuration**
   - Set up PingID for multi-factor authentication
   - Configure MFA policies for different user groups
   - Create authentication flows with step-up authentication
   - Test MFA for remote access scenarios
   - Document MFA implementation and user guides

Mid-Level Tasks

1. **Advanced Authentication Policies**
   - Implement adaptive authentication rules
   - Configure risk-based authentication policies
   - Create contextual authentication flows
   - Set up device-based authentication requirements
   - Document the complete authentication policy framework

2. **PingDirectory Implementation**
   - Configure PingDirectory as a user directory
   - Set up data synchronization with AD
   - Create access control policies
   - Implement high availability configuration
   - Document directory services architecture

3. **API Security**
   - Configure PingAccess for API protection
   - Implement OAuth2 authorization server
   - Set up API access policies
   - Create custom OAuth scopes for healthcare APIs
   - Document the API security architecture

Senior Level Tasks

1. **Enterprise Ping Architecture**
   - Design a complete Ping Identity suite implementation
   - Create a federated identity architecture for healthcare partners
   - Implement a comprehensive authorization framework
   - Design a complete customer identity solution
   - Develop a security architecture document for the entire solution

ForgeRock Tasks

Junior Level Tasks

1. **ForgeRock Access Management Basics**
   - Install and configure ForgeRock Access Management
   - Set up connection to Active Directory
   - Create basic authentication trees
   - Configure password policies
   - Test basic authentication flows

2. **Application Integration**
   - Configure SAML2 federation for healthcare applications
   - Set up OAuth2/OIDC clients for modern applications
   - Create basic authorization policies
   - Test single sign-on flows
   - Document SSO implementation

3. **Multi-Factor Authentication**
   - Configure ForgeRock Authenticator for MFA
   - Set up push authentication
   - Create step-up authentication flows
   - Test MFA for sensitive applications
   - Document MFA implementation

Mid-Level Tasks

1. **Advanced Authentication Trees**
   - Create complex authentication trees with decision nodes
   - Implement risk-based authentication
   - Configure contextual authentication
   - Create device profile nodes
   - Document advanced authentication architecture

2. **ForgeRock Identity Management**
   - Configure IDM for identity lifecycle management
   - Set up automated provisioning workflows
   - Create custom connectors for healthcare applications
   - Implement role-based provisioning rules
   - Document the complete identity lifecycle architecture

3. **Directory Services**
   - Configure ForgeRock Directory Services
   - Implement replication for high availability
   - Set up data synchronization with AD
   - Create access control instructions
   - Document directory services architecture

Senior Level Tasks

1. **Enterprise ForgeRock Architecture**
   - Design a comprehensive IAM solution with the ForgeRock platform
   - Create a zero trust architecture using ForgeRock components
   - Implement a complete authorization framework
   - Design custom healthcare-specific authentication journeys
   - Develop a complete identity platform strategy document

Integration-Focused Tasks

Mid-Level Tasks

1. **Multi-Platform Integration**
   - Configure Azure AD for cloud identity and CyberArk for privileged access
   - Implement SailPoint for governance and Okta for authentication
   - Create integrated workflows across platforms
   - Document the complete multi-platform architecture
   - Design authentication workflows across systems

2. **Healthcare-Specific Integrations**
   - Configure Epic EHR integration with IAM platforms
   - Implement e-prescribing system integration with DEA-compliant authentication
   - Set up patient portal access with appropriate identity verification
   - Create pharmacy system integration with role-based access
   - Document healthcare application integration architecture

Senior Level Tasks

1. **Comprehensive IAM Program**
   - Design an IAM reference architecture using multiple platforms
   - Create a strategic IAM roadmap with platform selection criteria
   - Develop governance processes spanning multiple IAM solutions
   - Design migration strategies between platforms
   - Create comprehensive security and compliance frameworks

Implementation Recommendations

To maximize your weekend lab experience:

1. **Choose 2-3 Platforms**: Rather than trying to cover all platforms, focus on 2-3 that interest you most (I recommend Azure AD and CyberArk as good starting points)

2. **Setup Free Trials/Dev Instances**:

   - Azure AD: Use a free trial Microsoft 365 tenant
   - Okta: Sign up for a free developer account
   - SailPoint: Look for virtual labs or demos
   - CyberArk: Check for free trials or lab environments
   - Ping Identity: Use developer accounts
   - ForgeRock: Access developer resources

3. **Progress Through Levels**:
   - Start with basic connectivity and authentication tasks
   - Move to application integration
   - Progress to more advanced governance scenarios

4. **Document Your Work**:
   - Take screenshots of your configurations
   - Create architecture diagrams
   - Write procedure documents as if for TrustCare
   - Build a portfolio demonstrating your IAM platform knowledge

5. **Create a Hybrid Scenario**:
   - Show how TrustCare would use Azure AD for cloud identity
   - Integrate with CyberArk for privileged access
   - Demonstrate how these systems would work together

These platform-specific tasks, combined with your Active Directory work in the TrustCare scenario, will give you comprehensive experience that directly addresses all aspects of the Junior IAM Engineer role at Xtensys, including the platform experience requirement.