**HiLCoE**

School of Computer Science and Technology

Unix Systems Administration (CS362)

Unix System Administration Procedures for Commercial Bank of Ethiopia(CBE)

Name: Kalab Dereje

ID:WB4707

Section: A

Submitted To: Ashenafi Kassahun

Unix administrators in financial institutions play a crucial role in managing the Unix-based infrastructure that supports various critical financial applications and services. The specific responsibilities and tasks of Unix administrators in financial institutions can vary depending on the size and complexity of the organization's IT environment. Here are some common aspects of Unix administration in CBE financial institutions:

1. Server Management

* Provisioning, configuring, and maintaining Unix servers that host financial applications and databases.
* Ensuring server security, including applying patches and updates to protect against vulnerabilities.

2. Performance Tuning

* Monitoring server performance and resource utilization to ensure optimal performance of financial systems.
* Identifying and resolving performance bottlenecks.

3. Data Security and Compliance

* Implementing and enforcing security policies and access controls to protect sensitive financial data.
* Ensuring compliance with industry-specific regulations (e.g., PCI DSS, SOX) and security standards.

4. Backup and Recovery

* Establishing and maintaining robust backup and disaster recovery strategies to protect financial data.
* Regularly testing and verifying backup and recovery procedures.

5. User Management

* Managing user accounts, permissions, and access to financial applications and data.
* Monitoring user activity for security and compliance purposes.

6. Patch Management

* Applying software patches, updates, and security fixes to Unix systems in a timely manner to address vulnerabilities and maintain system stability.

7. Scripting and Automation

* Developing and maintaining scripts and automation tools to streamline administrative tasks and ensure consistency.
* Automating routine tasks like log rotation, report generation, and system monitoring.

8. High Availability

* Implementing high availability and fail over solutions to minimize downtime for critical financial applications.
* Ensuring business continuity in the event of hardware or software failures.

9. Monitoring and Logging

* Setting up monitoring tools to proactively detect issues and anomalies in the Unix environment.
* Managing log files for auditing and troubleshooting purposes.

10. Vendor and Third-Party Software Management

* Coordinating with software vendors to ensure proper licensing and support for financial applications running on Unix systems.
* Managing software installations and updates.

11. Capacity Planning

* Monitoring resource usage trends and planning for future capacity needs.
* Recommending hardware upgrades or additional servers as necessary.

12. Incident Response and Troubleshooting

* Responding to and resolving system incidents, including outages and performance issues.
* Conducting root cause analysis and implementing preventive measures.

13. Documentation and Training

* Maintaining documentation of system configurations, procedures, and best practices.
* Providing training and knowledge transfer to other IT staff members.

1. Security Audits and Penetration Testing

* Collaborating with security teams to conduct security audits and penetration testing to identify and address vulnerabilities.

15. Disaster Recovery Planning

* Developing and regularly updating disaster recovery plans and procedures to ensure business continuity in the event of a major disruption.

Unix administrators in financial institutions must be highly skilled, detail-oriented, and capable of working under strict security and compliance requirements. They play a critical role in safeguarding financial data and ensuring the smooth operation of financial systems.

Implementing Unix system administration procedures for Commercial Bank of Ethiopia, requires careful planning, well-defined policies, and effective strategies to ensure the security, reliability, and compliance of the Unix-based systems that underpin the bank's operations.

**Plan**

1. Assessment and Inventory

* Conduct a comprehensive assessment of the existing Unix infrastructure, including hardware, software, and network configurations.
* Create an inventory of all Unix servers, their roles, and dependencies.

2. Stakeholder Analysis

* Identify key stakeholders, including IT teams, management, and compliance officers, who will be involved in or affected by the Unix administration procedures.

3. Risk Assessment

* Perform a risk assessment to identify potential security vulnerabilities and compliance risks in the Unix environment.

4. Goals and Objectives

* Define clear goals and objectives for the Unix system administration procedures, such as enhancing security, ensuring compliance, and improving system performance.

5. Resource Allocation

* Determine the resources needed for effective Unix administration, including personnel, hardware, software, and training.

6. Timeline and Milestones

* Develop a timeline for implementing the procedures and establish milestones to track progress.

**Policies**

1. Security Policies

* Establish comprehensive security policies covering access controls, encryption, authentication, and intrusion detection for Unix systems.
* Define password policies and user account management procedures.
* Implement firewall rules and network security policies to protect Unix servers.

2. Compliance Policies

* Ensure that the Unix administration procedures align with relevant financial industry regulations and standards.
* Define procedures for regular compliance audits and reporting.

3. Backup and Recovery Policies

* Develop backup and recovery policies that include data backup schedules, retention periods, and disaster recovery plans.

4. Change Management Policies

* Implement change management policies to control and document changes made to Unix systems, including software updates and configurations.

5. Incident Response Policies

* Establish procedures for identifying, reporting, and responding to security incidents and breaches on Unix servers.

6. Monitoring and Logging Policies

* Define policies for monitoring system performance and security events on Unix servers.
* Ensure that logs are properly configured and retained for auditing purposes.

**Strategies**

1. Security Strategy

* Develop a multi-layered security strategy that includes firewalls, intrusion detection systems, and regular vulnerability assessments.

2. Training and Skill Development

* Invest in training and skill development for Unix administrators to keep them updated on the latest security threats and best practices.

3. Automation and Scripting

* Implement automation tools and scripting for routine tasks to improve efficiency and consistency.

4. Business Continuity and Disaster Recovery

* Develop strategies for business continuity and disaster recovery, including fail over systems and data replication.

5. Vendor and Third-Party Management

* Establish strategies for managing vendor relationships, including software and hardware suppliers, to ensure timely support and updates.

6. Regular Auditing and Testing

* Conduct regular security audits, penetration testing, and compliance assessments to identify and address vulnerabilities.

7. Documentation and Reporting

* Maintain detailed documentation of procedures, configurations, and incident reports.
* - Develop reporting mechanisms to keep management informed of system status and security posture.

8. Budget and Resource Allocation

* Allocate resources according to the bank's strategic priorities and risk assessments.

9. User Awareness and Training

* Develop strategies for educating bank employees about security best practices and their roles in maintaining system security.

It's important to know these plans, policies, and strategies specifically to the Commercial Bank of Ethiopia's unique requirements, regulatory environment, and risk profile. Additionally, involve relevant stakeholders and seek their input throughout the planning and implementation process to ensure alignment with the bank's objectives. Regularly review and update these procedures to adapt to changing security threats and compliance requirements.