evidence
action

Azure Linux Server Standard Operating Procedure (SOP) Manual

Evidence Action Inc. – Revision Date: January 22, 2024.

evidence action

Table of Contents

1.Introduction 3

1.1 Purpose of the SOP 3

1.2 Emphasis on Secure Access Management 3

1.3 SSH Key Rotation 3

1.4 Restricted Storage 3

2.Access Management 3

2.1 Access Request Procedure 3

2.1.1 Requesting Access 3

2.1.2 Required Information 4

2.2 Approval Authorization 4

2.2.1 Approval Process 4

3.Authentication and Authorization 5

3.1 SSH Key Management 5

3.1.1 Use of SSH Keys 5

3.1.2 Key Revocation 5

4.Responsibility Disaggregation 6

4.1 Infrastructure-related Activities 6

5.Security Best Practices 7

5.1 Do's 7

5.1.1 Regular Updates and Patches 7

5.1.2 Network Security Measures 7

5.2 Don'ts 7

5.2.1 Sharing of Private Keys 7

5.2.2 Disable SSH Key Authentication 7

5.2.3 Neglect Software Updates 7

6.Contact Information 7

1. Introduction

1.1 Purpose of the SOP

This SOP establishes guidelines and procedures for the secure management of access using SSH keys on our Azure Linux server hosting the corporate web server at Evidence Action Inc. It aims to ensure the confidentiality, integrity, and availability of our critical assets.

1.2 Emphasis on Secure Access Management

Secure access management is vital to protect sensitive data and maintain the operational integrity of our corporate web server. This SOP focuses on the meticulous use and management of SSH keys as a robust authentication mechanism.

1.3 SSH Key Rotation

To enhance security, SSH keys will be rotated every 90 days.

1.4 Restricted Storage

SSH keys must not be stored outside the scope of Evidence Action Inc. infrastructure. Any external storage or sharing of keys is strictly prohibited.

2. Access Management

2.1 Access Request Procedure

2.1.1 Requesting Access

Employees or external parties including consultants or vendors seeking access to the corporate web server must adhere to the following process:

1. **Access Request Form Submission:**
    - Complete the Access Request Form providing necessary details, including employee information and project details.
2. **SSH Key Generation and Submission:**
    - Generate SSH key pairs securely through the Microsoft Azure portal, official documentation on how to create a SSH Key: HERE
    - Submit the generated SSH keys through the designated channel using a Google Drive shared link, this link must be created with a 48-hour expiration time.
    - After granting or revoking access, a ticket must be sent at helpdesk@evidenceaction.org to inform the IT Department.

2.1.2 Required Information

Access requests should encompass the following information:

- Personal details (name, department, contact information)
- Project information (description, duration)

2.2 Approval Authorization

2.2.1 Approval Process

Access requests undergo a meticulous approval process:

1. **Reviewer Role:**
    - The designated Reviewer Role reviews access requests based on project relevance and security clearance.
        - Name: Luis Maradiaga
        - Position: IT Consultant
        - Email: luis.maradiaga@evidenceaction.org
2. **Approval Team:**
    - An Approval Team ensures compliance with access criteria and project requirements.
        - Name: Allen Rozario
        - Position: Global IT Director
        - Email: allen.rozario@evidenceaction.org
3. **IT Support Implementation:**
    - Upon approval, the IT support team implements the necessary access configurations.
        - Name: Luis Maradiaga
        - Position: IT Consultant
    - Email: luis.maradiaga@evidenceaction.org

3. Authentication and Authorization

3.1 SSH Key Management

3.1.1 Use of SSH Keys

SSH keys serve as the primary method for user authentication:

2. **Key Generation:**
    - Generate SSH key pairs securely through the Microsoft Azure portal, official documentation on how to create a SSH Key: HERE
3. **Distribution:**
    - Distribute the generated SSH keys through the designated channel using a Google Drive shared link, this link must be created with a 48-hour expiration time.
    - After granting access, a ticket must be sent at helpdesk@evidenceaction.org to inform the IT Department.
4. **Revocation Process:**
    - In case of lost keys or terminated access, follow the key revocation process outlined in the Key Revocation Procedure.

3.1.2 Key Revocation

Lost keys or terminated access requires prompt action:

1. **Change Management Form Completion**
    - The Change Management Form must be filled out and completed when terminating access to the server, following the same Approval workflow.
2. **Access Revocation:**
    - Execute the key revocation process to maintain a secure access environment, this should be done on the Microsoft Azure Portal.
3. **Reporting:**
    - After revoking access, a ticket must be sent at helpdesk@evidenceaction.org to inform the IT Department, a digital copy of the Change Management Form needs to be attached.

4. Responsibility Disaggregation

Ensuring an effective allocation of responsibilities is paramount for streamlined operations. Therefore, we advocate for a clear and distinct division of tasks:

4.1 Infrastructure-related Activities

The execution of tasks concerning the server's foundational systems, including configuration, maintenance, and security, falls within the purview of the **IT Department exclusively**. This encompasses critical functions such as:

- Server Operating System Configuration and Maintenance
- Database server configuration and Maintenance.
- Network Setup and Monitoring
- Server Operating System Security Patching and Updates
- Firewall Configuration
- User Access Control

4.2 Craft CMS (Content Management System) Related Activities

Activities associated with Craft CMS (Content Management System), are well-suited for **external consultants**. These activities may include:

- Website Content Updates
- Plugin Installations and Updates
- Theme Customization
- Performance Optimization
- Routine Website Checks

In instances where an infrastructure-related task necessitates the involvement of an external consultant, we kindly request adherence to our standard approval process. This entails submitting a detailed request through the Access Request Form, accompanied by clear justifications for the external consultant's involvement. The request will undergo the established approval workflow to ensure alignment with our security and operational standards.

5. Security Best Practices

5.1 Do's

5.1.1 Regular Updates and Patches

Ensure the Azure Linux server remains up to date:

1. **Regular Patching:**
    - Schedule regular updates and patches to be applied every 30 days.
2. **Testing Environment:**
    - Test updates in a designated staging environment before applying to production.

5.1.2 Network Security Measures

Implement comprehensive network security measures:

1. **Firewalls:**
    - Configure and maintain firewalls to control incoming and outgoing network traffic, this should be monitored using the Microsoft Azure Network Configuration and Cloudflare control panel.

5.2 Don'ts

5.2.1 Sharing of Private Keys

Strictly prohibit the sharing of private SSH keys or access credentials:

5.2.2 Disable SSH Key Authentication

Avoid unauthorized disabling of SSH key authentication:

5.2.3 Neglect Software Updates

Maintain diligence in software updates and patches.

6. Contact Information

If you encounter any issues or have further questions, please reach out to the IT Helpdesk for assistance at helpdesk@evidenceaction.org.