UDACITY

Data Security Analysis in Online Payment Processing

Benjámin Rácskai

23.06.2024

Project Scenario

Section One:
Data Governance

Strategic Data Security Policies

IT Staff should perform a data classification annually, or when there are notable business or technology changes.

Data Security:

- **Enhanced Protection:** By classifying data, IT staff can identify which data is sensitive and needs higher protection. This ensures that critical information is secured with appropriate controls.
- **Prioritization:** Allows the organization to prioritize security efforts on the most valuable or vulnerable data, reducing the risk of data breaches.

Compliance:

- **Regulatory Adherence:** Many regulations require organizations to classify their data to ensure compliance with data protection laws (e.g., GDPR, CCPA). Regular classification helps maintain compliance and avoid legal penalties.

Risk Management:

- **Risk Identification:** Classification helps in identifying data-related risks by understanding the type and sensitivity of data stored. This can inform risk mitigation strategies.
- **Incident Response:** In case of a data breach, knowing the classification of compromised data helps in assessing the impact and responding appropriately.

Operational Efficiency:

- **Resource Allocation:** Proper data classification ensures resources are allocated efficiently by focusing on protecting the most critical data.
- **Streamlined Processes:** Helps in creating streamlined processes for handling different types of data, improving overall efficiency and reducing unnecessary work.

Strategic Data Security Policies

IT Staff should perform an application and critical system classification annually, or when there are notable business or technology changes.

Data Security:

- **Improved Security Posture:** Classifying applications and critical systems helps identify which systems are most vital to business operations and require stronger security measures.
- **Vulnerability Management:** Knowing which systems are critical can lead to more focused vulnerability assessments and timely patching, enhancing security.

Compliance:

- **Regulatory Requirements:** Certain regulations require organizations to identify and secure critical systems. Regular classification ensures compliance with these requirements.

Risk Management:

- **Business Continuity:** Identifying critical systems supports business continuity planning by ensuring that essential applications are protected and can be restored quickly in case of disruption.
- **Threat Assessment:** Helps in assessing potential threats to key systems and prioritizing them in risk management plans.

Operational Efficiency:

- **System Prioritization:** Allows IT to prioritize maintenance and updates for the most critical systems, reducing downtime and enhancing reliability.
- **Resource Optimization:** Ensures resources are focused on maintaining and securing essential applications, improving overall IT efficiency.

Strategic Data Security Policies

IT Staff should perform a regulatory assessment annually, or when there are notable business or technology changes.

Data Security:

- **Compliance-Based Security:** A regulatory assessment ensures that security measures align with current regulatory requirements, which often encompass industry best practices for data protection.
- **Proactive Security Measures:** Helps in identifying and addressing security gaps before they become compliance issues, enhancing overall security.

Compliance:

- **Up-to-Date Compliance:** Ensures the organization remains compliant with evolving regulations, avoiding fines and legal issues.
- **Audit Preparedness:** Regular assessments make it easier to prepare for audits by maintaining up-to-date records and demonstrating compliance.

Risk Management:

- **Regulatory Risk Mitigation:** Identifies regulatory risks and provides a framework for addressing them, reducing the likelihood of compliance-related incidents.
- **Strategic Planning:** Informs strategic planning by identifying new or changing regulatory requirements that may impact business operations.

Operational Efficiency:

- **Consistent Processes:** Regular assessments ensure consistent application of compliance-related processes across the organization, reducing errors and inefficiencies.
- **Continuous Improvement:** Promotes a culture of continuous improvement by regularly evaluating and updating compliance practices.

Data Classification

Confidential: It includes data that is highly sensitive and whose unauthorized disclosure could cause significant harm to the company, its employees, or its customers. Access to confidential data should be highly restricted and protected with strong security measures. Examples include personally identifiable information (PII), financial data, and intellectual property.
Internal: It includes data that is meant for internal use within the company and whose unauthorized disclosure might cause moderate harm. While not as sensitive as confidential data, internal data should still be protected and only accessible by employees who need it to perform their duties. Examples include internal communications and operational information.
Public: It includes data that is intended for public consumption or that, if disclosed, would cause minimal or no harm to the company. Public data can be freely shared and accessed without any significant security measures. Examples include marketing materials and published blogs.

Categorize each dataset into one of the three data types

Dataset	Data Type
Employee profile data	Confidential
Customer profile data	Confidential
Company email	Internal
Repository of previously published blogs	Public
Internal employee newsletters	Internal
Technology engineering diagrams	Confidential
Intellectual property	Confidential

Data Regulations

Confidential	GDPR, CCPA, PCI DSS, SOX : GDPR applies if any data subject is an EU resident, while CCPA applies to residents of California. PCI DSS applies if the data includes payment information. SOX is relevant for financial data and controls, particularly if employees are involved in financial reporting processes.
Internal	SOX, Corporate Policies and Standards, NIST : SOX is relevant for ensuring that any internal communications related to financial reporting are accurate and protected. Corporate policies ensure that internal data is used and managed according to the company's standards. NIST guidelines help in creating a secure framework for handling and protecting internal communications.
Public	Copyright Laws, Corporate Policies and Standards : Comply with copyright laws to protect the company's intellectual property and avoid legal issues. Corporate policies ensure that public content maintains the company's image and adheres to communication standards.

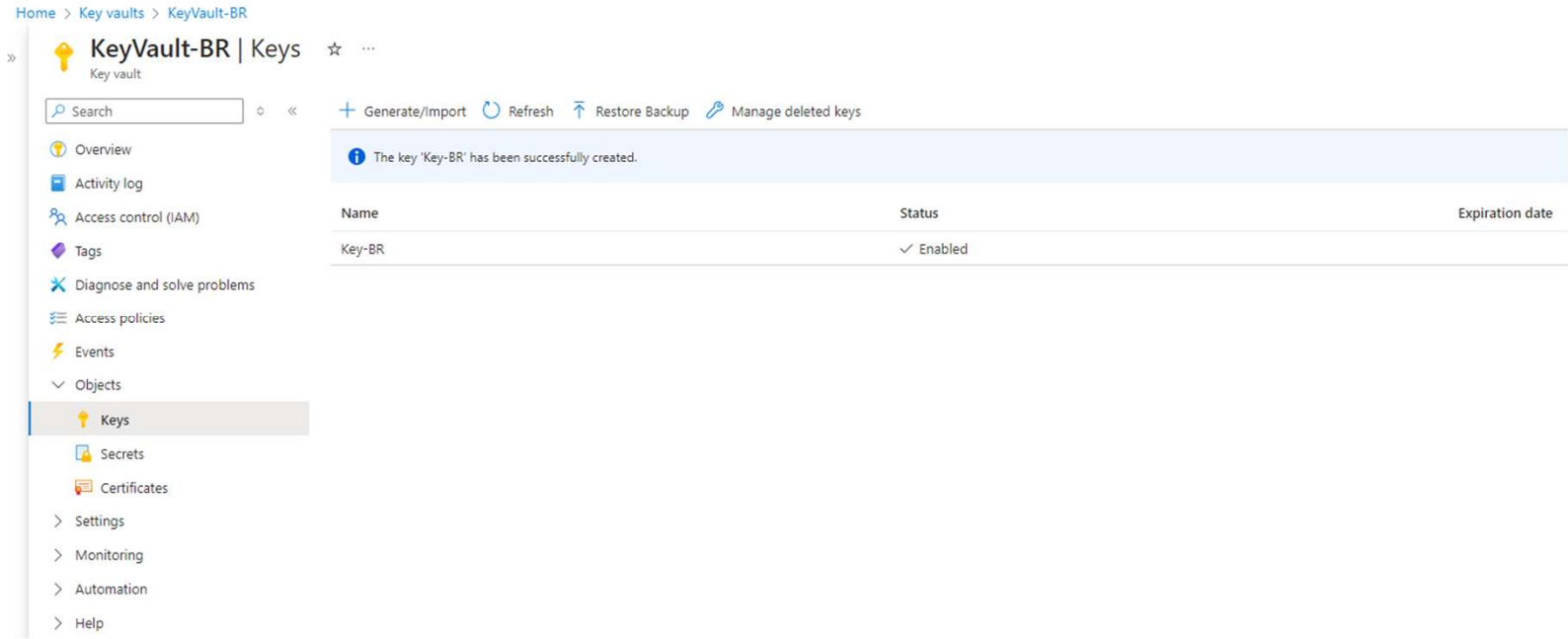
Regulatory Compliance

Data Encryption: All confidential and sensitive data, including employee profile data, customer profile data, technology engineering diagrams, and intellectual property, must be encrypted both in transit and at rest using industry-standard encryption protocols. This policy applies to all systems, databases, and devices that store, process, or transmit confidential and sensitive data.
Access Control: Access to confidential and internal data must be restricted based on the principle of least privilege. Role-based access control (RBAC) must be implemented to ensure that users only have access to the data necessary for their job functions. This policy applies to all employees, contractors, and third parties with access to the company's information systems.
Data Disposal: Confidential and internal data must be securely disposed of when no longer needed. Physical media must be shredded or incinerated, and electronic data must be permanently deleted using approved data sanitization methods. This policy applies to all physical and electronic media that store confidential or internal data.
Breach Notification: In the event of a data breach involving confidential or internal data, the Data Security Analyst must notify affected parties and relevant regulatory authorities within 72 hours of discovering the breach, in accordance with GDPR and CCPA requirements. This policy applies to all incidents of data breaches involving the company's information systems.
Security Awareness Training: All employees must undergo mandatory security awareness training upon hire and annually thereafter. Training must cover topics such as data protection regulations, phishing, password management, and incident reporting. This policy applies to all employees, contractors, and third parties with access to the company's information systems.
Data Backup and Recovery: Confidential and internal data must be regularly backed up, and backup copies must be stored securely offsite. A disaster recovery plan must be in place to ensure the timely restoration of data and services in the event of a disruption. This policy applies to all systems and applications that store or process confidential or internal data.

Section Two:
Data Confidentiality

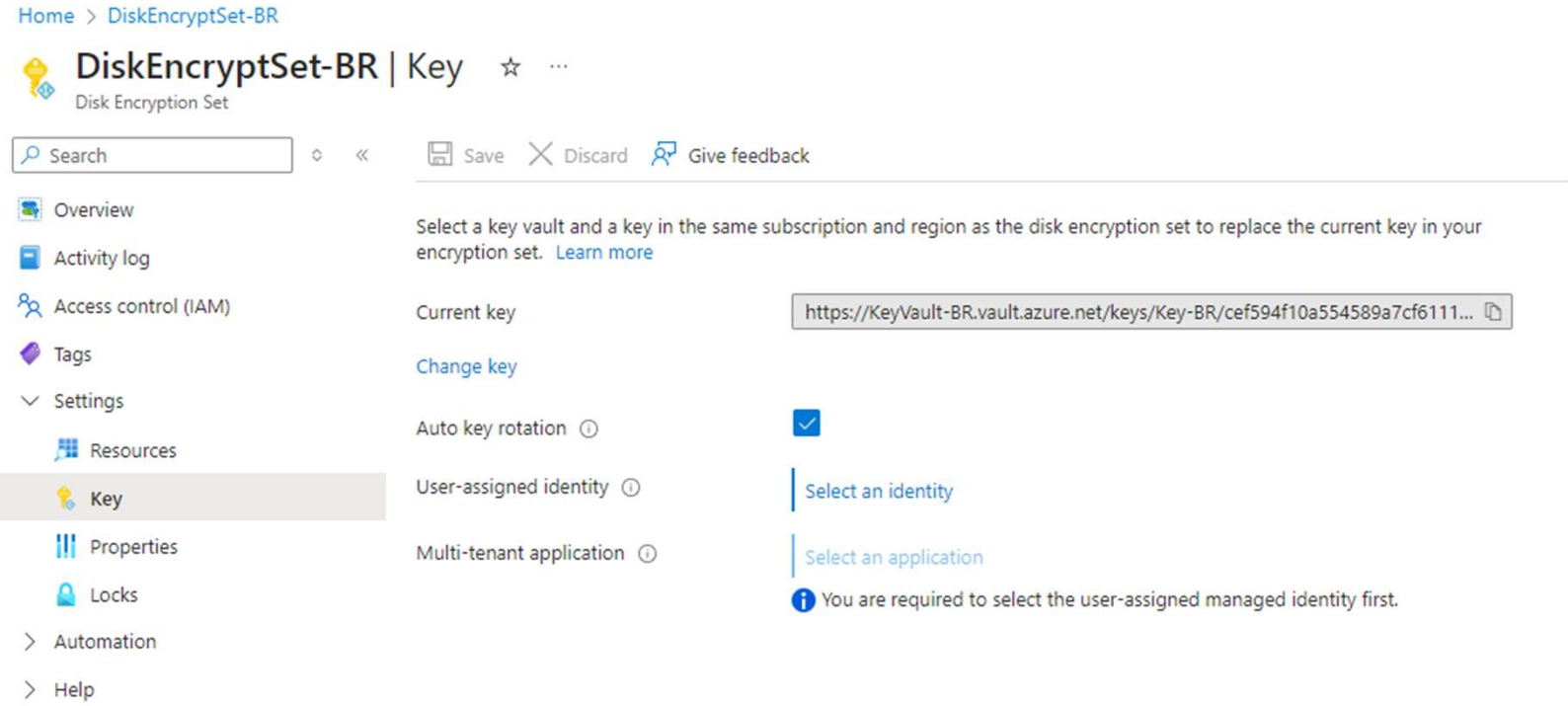
Securing Disks

Place the screenshot from the Keys page of the Key Vault you created, with the generated key.



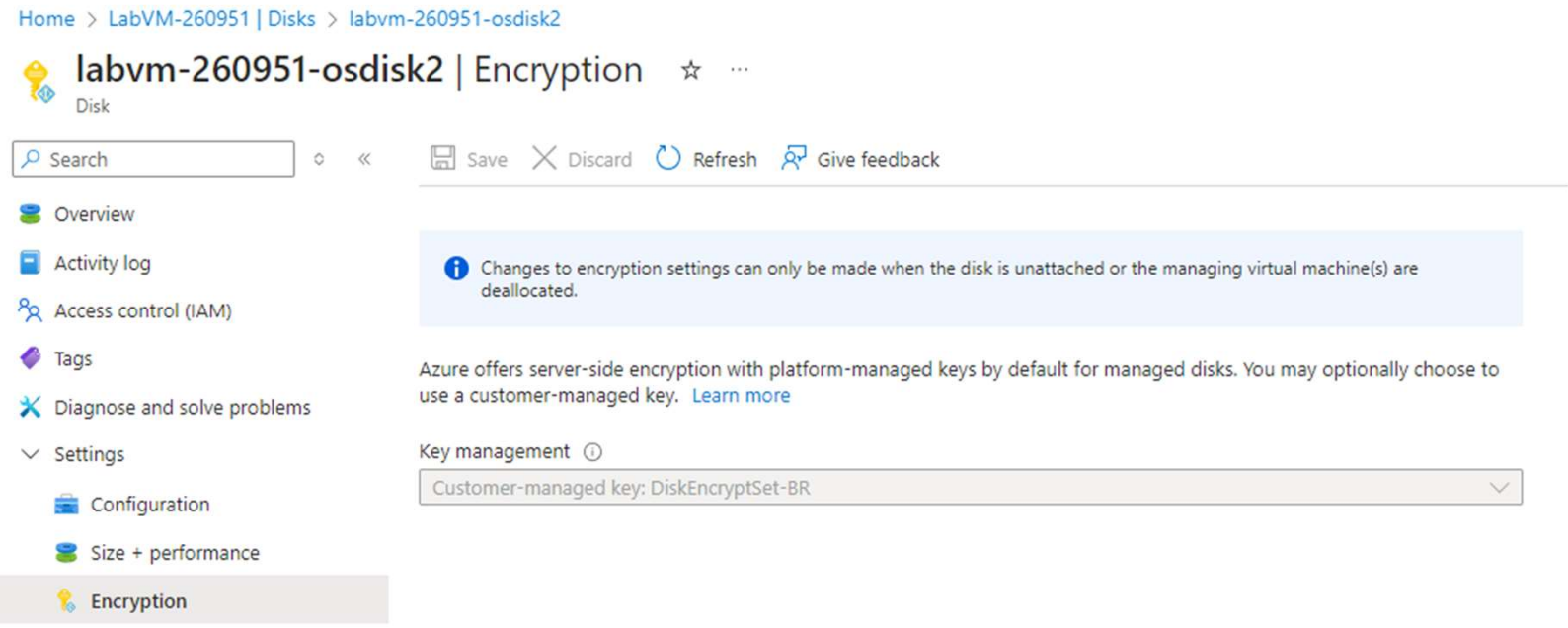
Securing Disks

Place the screenshot from Key page of the Disk Encryption Set you created



Securing Disks

Place the screenshot from the Encryption page of the Disk you created



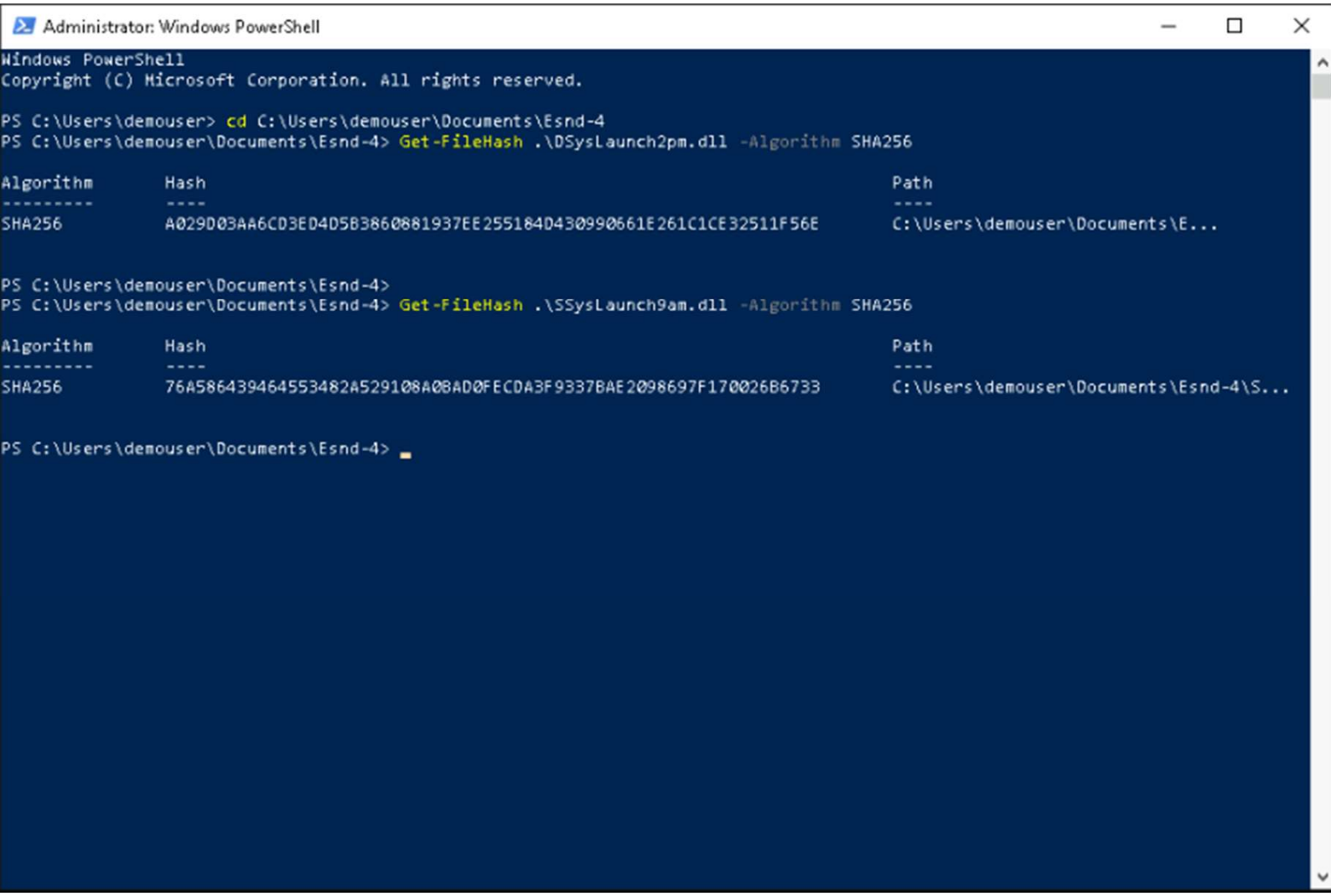
Section Three: Data Integrity

File Integrity Verification

The original DSysLaunch2pm.dll hash: B029D03AA6CD3ED4D5B3860881937EE255184D430990661E261C1CE3251184D4
The original SSysLaunch9am.dll hash: 76A586439464553482A529108A0BAD0FECDA3F9337BAE2098697F170026B6733

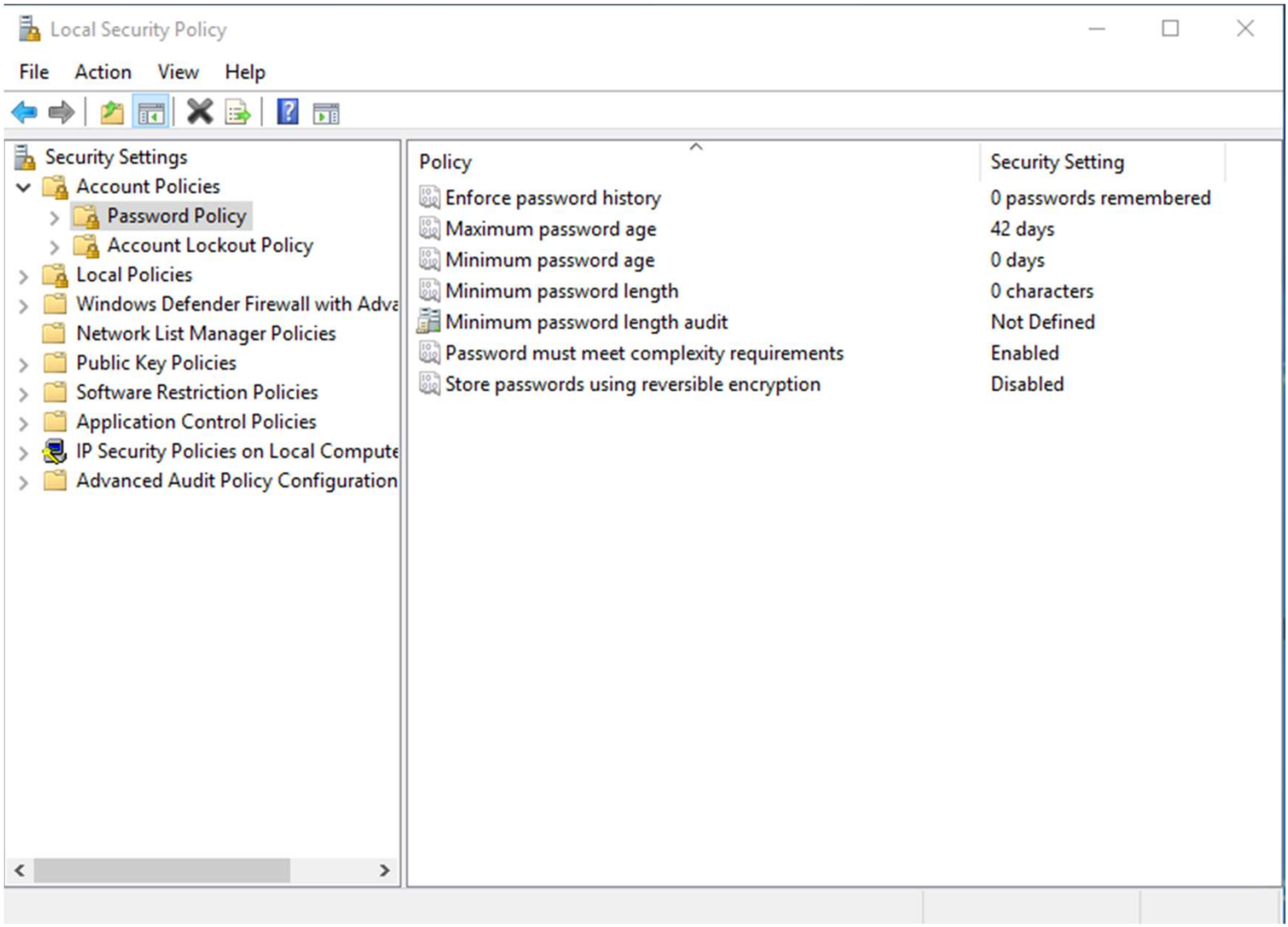
After generate hash to files:

1. DSysLaunch2pm.dll file: The two hashes are different which means the file changed.
2. SSysLaunch9am.dll file: The two hashes are same which means the file didn't changed.



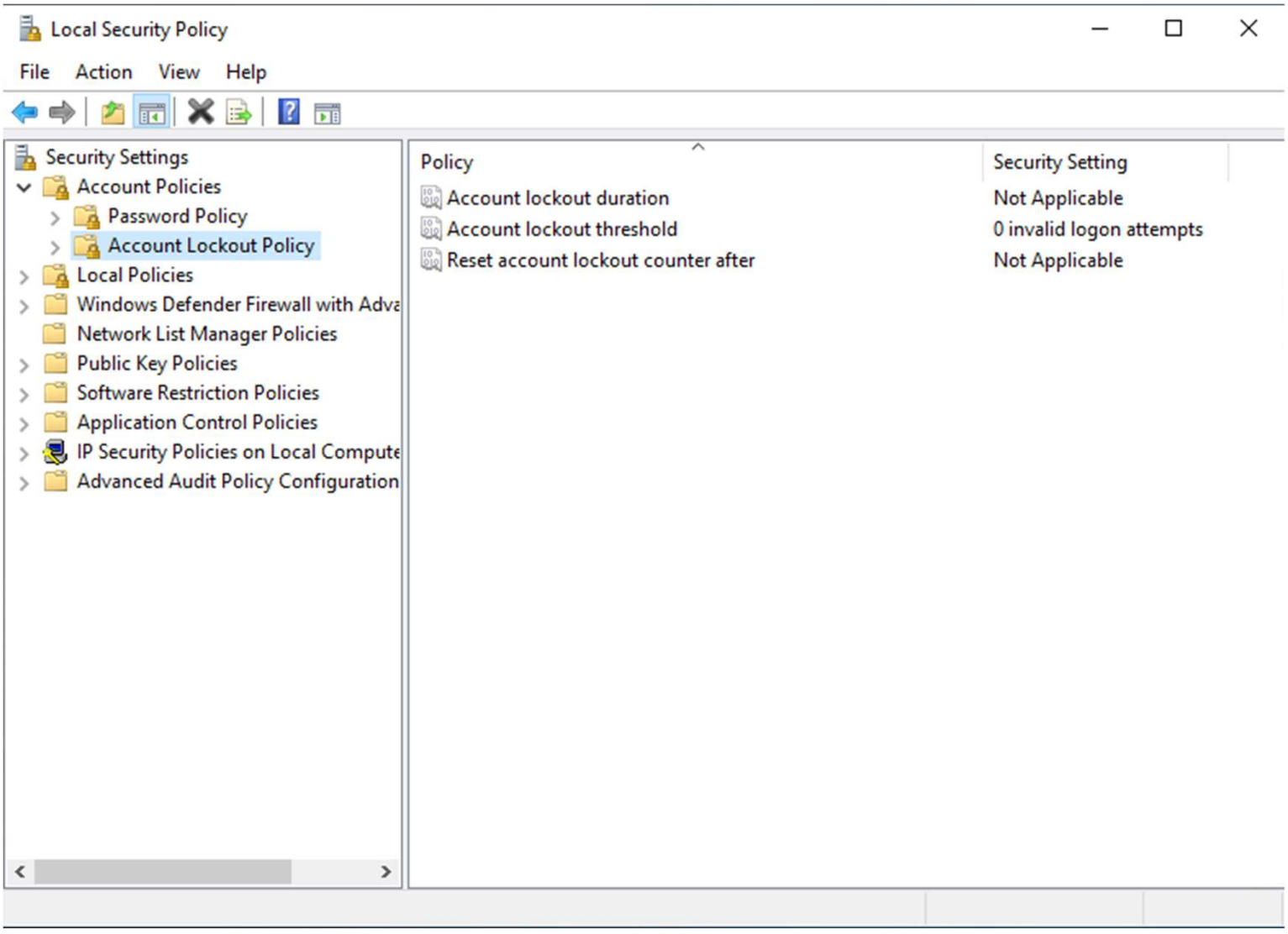
Auditing Security Settings

Place the screenshot of the password policy screen here



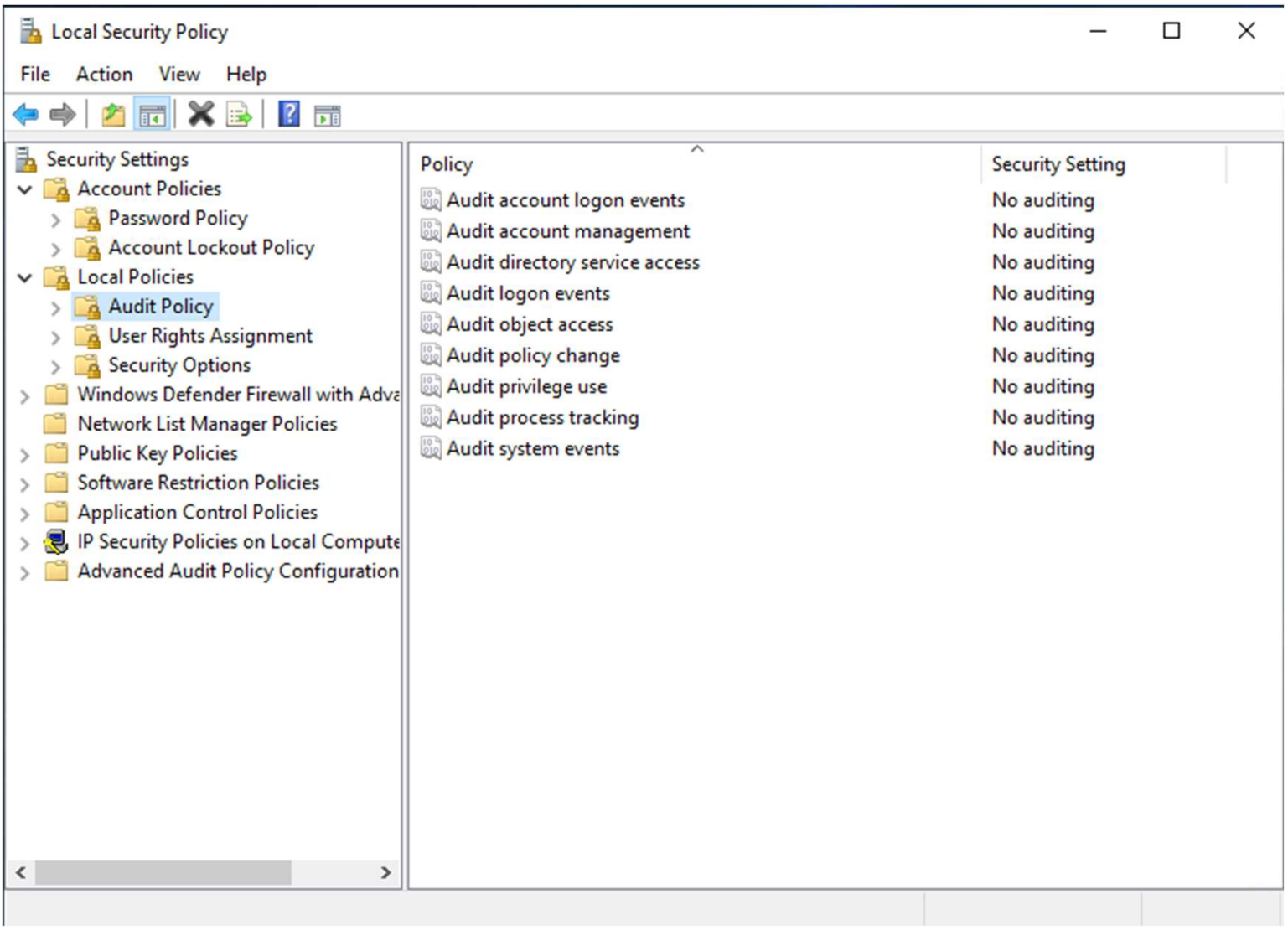
Auditing Security Settings

Place the screenshot of account lockout policy screen here



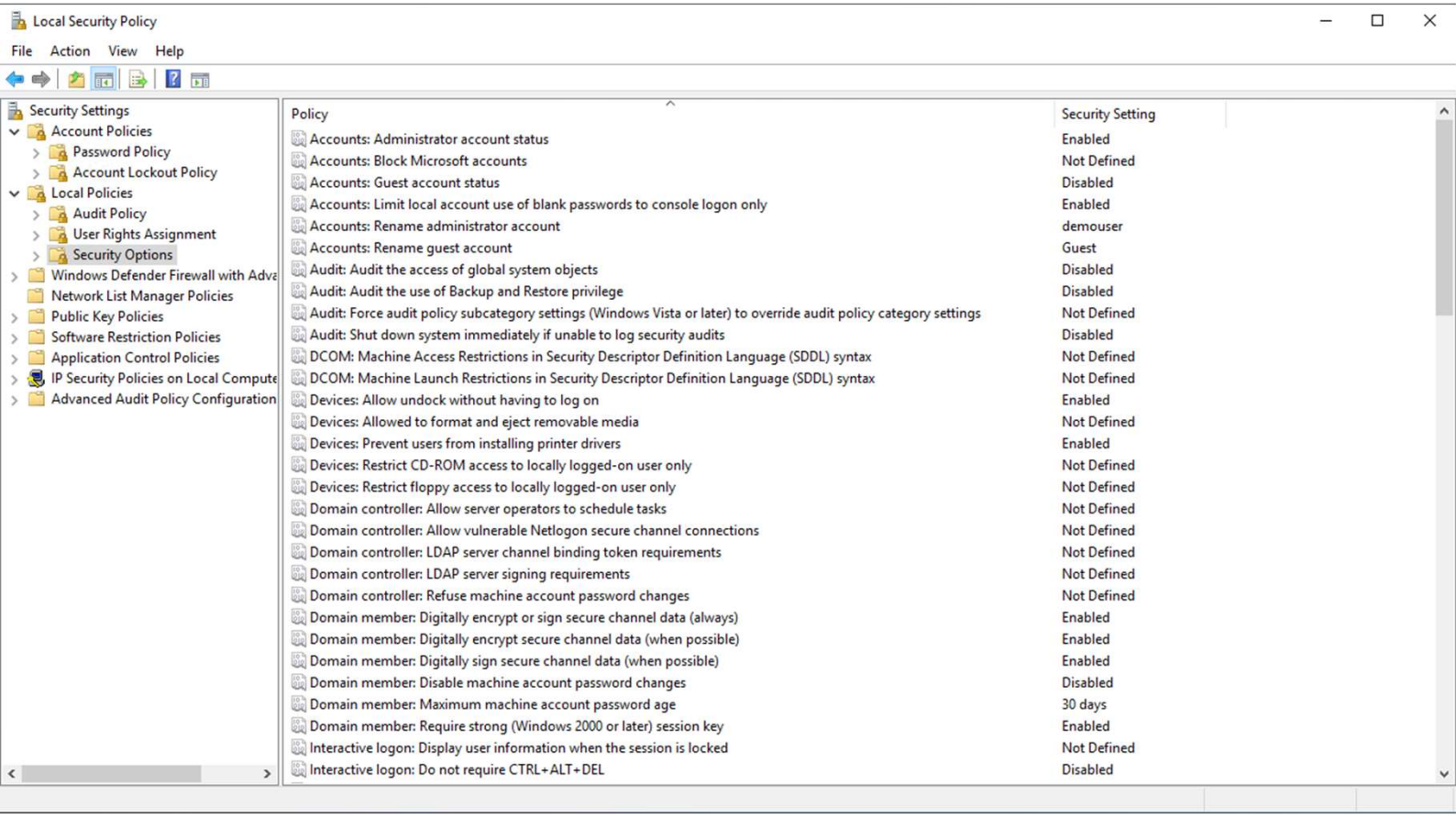
Auditing Security Settings

Place the screenshot of the audit policy screen here



Auditing Security Settings

Place the screenshot of the security options screen here



Enhancing VM Security

1. Minimum password length

Setting a minimum password length is a crucial security measure that ensures passwords are complex enough to resist brute force and dictionary attacks. Short passwords are more vulnerable to these attacks because they have fewer possible combinations. Industry best practices recommend a minimum password length of at least 8 characters.

Benefits:

Increases the number of possible password combinations, making brute force attacks more difficult.

Encourages users to create more complex passwords, reducing the likelihood of using easily guessable passwords.

Enhances overall security posture by making it harder for attackers to gain unauthorized access.

2. Account lockout threshold

The account lockout threshold setting specifies the number of failed login attempts allowed before an account is locked. This helps prevent automated attacks, such as brute force attempts, by limiting the number of guesses an attacker can make. Industry standards often recommend setting a threshold that balances security and usability, typically around 3-5 failed attempts.

Benefits:

Protects accounts from brute force attacks by limiting the number of password guesses.

Alerts administrators to potential unauthorized access attempts, allowing for timely investigation and response.

Reduces the risk of compromised accounts due to repeated login attempts with guessed or stolen credentials.

Enhancing VM Security

3. Account lockout duration

The account lockout duration defines how long an account remains locked after reaching the lockout threshold. Setting a reasonable duration (e.g., 15-30 minutes) ensures that genuine users who mistakenly enter their password multiple times are not permanently locked out, while still deterring attackers. This duration should balance security needs and user convenience.

Benefits:

Provides a deterrent to attackers by making automated attacks time-consuming and less likely to succeed.

Minimizes disruption to legitimate users by allowing them to regain access after a short period.

Reduces administrative overhead associated with unlocking accounts manually.

4. Audit logon events

Auditing logon events is a critical security practice that involves recording successful and failed login attempts. This enables organizations to monitor and analyze login activities, identify suspicious behavior, and respond to potential security incidents. Comprehensive logging and regular review are key components of security best practices and compliance requirements.

Benefits:

Helps detect unauthorized access attempts and potential security breaches.

Provides a forensic trail for investigating security incidents and understanding the scope of breaches.

Aids in compliance with regulatory requirements (e.g., GDPR, HIPAA) that mandate logging and monitoring of access to sensitive information.

Enables proactive security measures by identifying and responding to patterns of suspicious activity.

Section Four: Data Availability

Developing a Data Backup Strategy

Confidential Data	
Backup Frequency:	Daily
Retention Period:	1 Year
Confidential data, such as employee profile data, customer profile data, technology engineering diagrams, and intellectual property, are critical to the business and often subject to strict regulatory requirements. Daily backups ensure that any changes are quickly captured and can be restored in case of data loss or corruption. Industry best practices recommend frequent backups for highly sensitive information to minimize data loss. Retaining backups for one year aligns with many regulatory requirements that mandate the preservation of sensitive information for audit and compliance purposes. Additionally, a one-year retention period helps in recovering from data loss incidents that might not be immediately detected.	
Internal Data	
Backup Frequency:	Weekly
Retention Period:	90 Days
Internal data, including company emails and internal employee newsletters, are important but not as critical as confidential data. Weekly backups strike a balance between resource usage and data protection, ensuring that recent internal communications and updates can be recovered without overwhelming storage resources. A 90-day retention period is sufficient for internal data, as it allows the organization to restore recent internal communications and operational information while keeping storage manageable.	

Developing a Data Backup Strategy

Public Data	
Backup Frequency:	Monthly
Retention Period:	30 Days
Public data, such as previously published blogs, are least critical in terms of security and regulatory compliance. Monthly backups are sufficient to capture any updates or changes while minimizing the use of backup resources. Public data changes infrequently, so less frequent backups are appropriate. A 30-day retention period for public data backups is generally adequate, as these data are already publicly available and can be easily recreated or retrieved from other sources. Keeping backups for a short period reduces storage costs and complexity.	

Creating a Backup

Place the screenshot of the LabVM Backup screen here