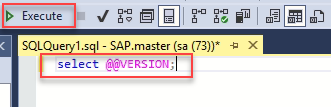
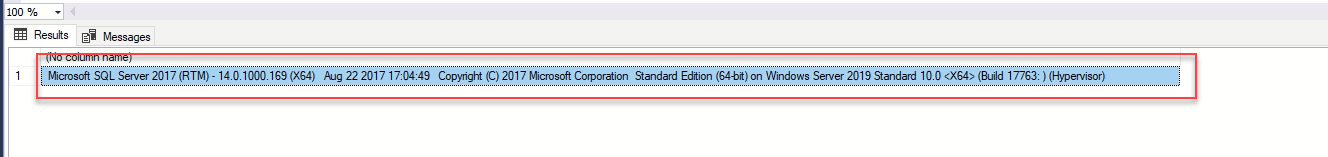
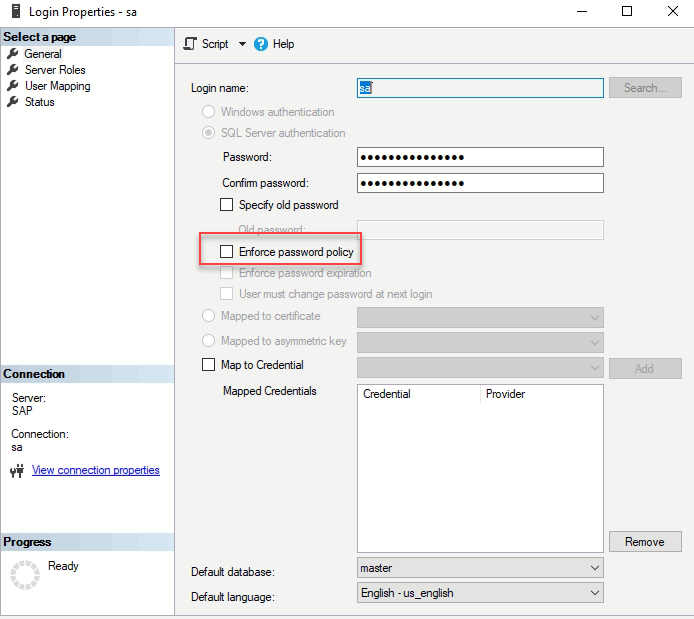
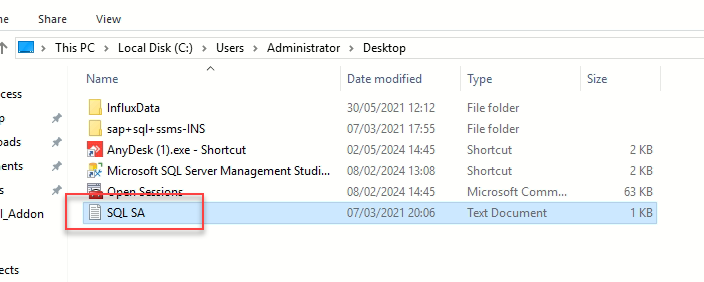
**Greetings,**

Today, we conducted a review of the SQL Server Examination on SAP Server, covering the following key points:

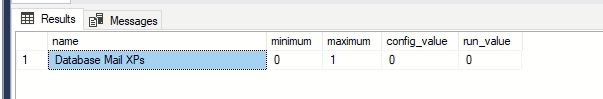
**1. Server Configuration:**

* **Network:** The server resides in a dedicated VLAN along with other servers, enhancing network segmentation.
* **Operating System:** Windows Server 2019
* 
* **SQL Server Version:** SQL Server Studio 18.6, (Note: This is not the latest version available for Windows Server 2019. An update is recommended.)
* 
* 

**2. SA User Account:**

* **Status**: The SA account is enabled, using a highly secure password with password policies enforced.
* **Issue Identified**: The SA password was found stored in plain text
* 
* **Action**: Remove the file containing the plain text password and store credentials securely in tools like KeePass or 1Password

**3. Database Mail XPs:**

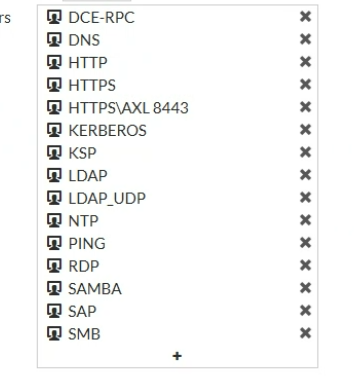
* Database Mail XPs are currently Disabled.
* 
* Command used to verify:

EXEC sp\_configure 'show advanced options', 1;

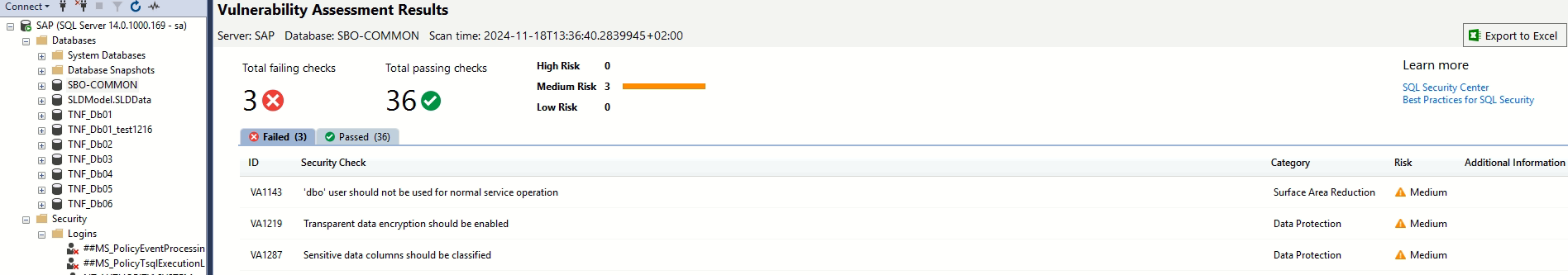
RECONFIGURE;

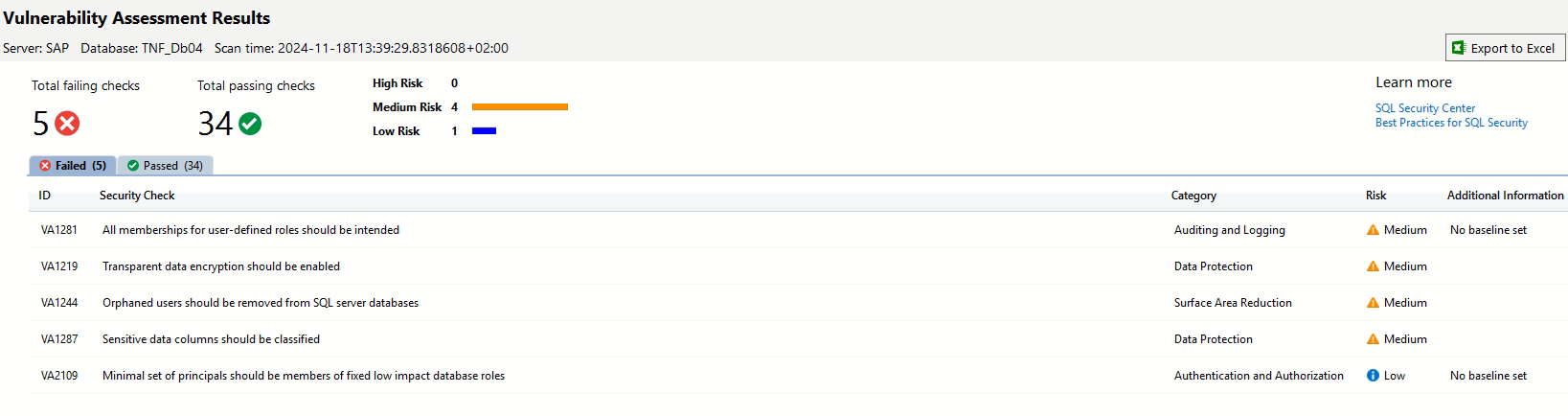
EXEC sp\_configure 'Database Mail XPs';

**4. SQL Server Traffic:**

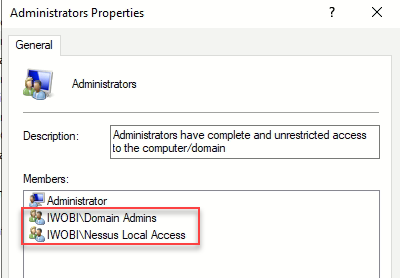
* **Firewall Rules:** Several rules are configured with SQL ports 1433 and 1434, with logs enabled on all rules.
* **Access:** all the VLAN2 has access to the SQL SAP Server with the following services, DNS,HTTP,HTTPS,Kerberos,KSP,LDAP,LDAP\_UDP,NTP,PING,RDP,SMABA,SAP,SMB.
* 
* **Action Required:** Verify the necessity of the relevant services, and recommended to lower down the people who have access to the SQL

**5. Database Vulnerability Assessment:**

* A vulnerability assessment was conducted on the databases.
* 
* A screenshot of a computer

  Description automatically generated
* 
* **Steps:**
  + Right-click on the database -> Tasks -> Vulnerability Assessment -> Scan for Vulnerabilities.
* **Next Steps:** Review and implement the remediation recommendations.

**6. Local Administrator Accounts:**

* A list of local administrators on the SQL Server was reviewed.
* 

**7. Server Internet Access:**

* The server currently has access to the internet.
* A screenshot of a computer program

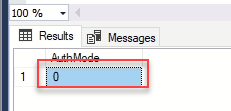
  Description automatically generated

**8. File Downloads and Server Security:**

* The server is not fully hardened, allowing drag-and-drop, copy-paste, and unrestricted downloads.
* **Recommendation:** Implement stricter security controls.

**9. Authentication Methods:**

* The server supports Windows and SQL Authentication.
* A close-up of a computer screen

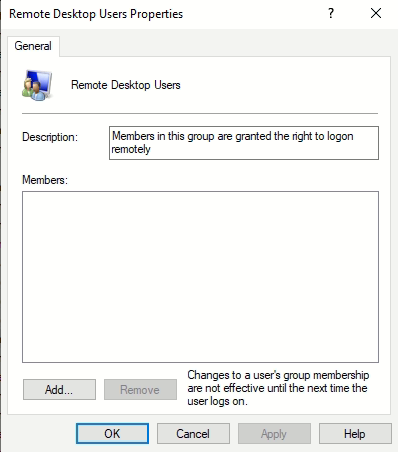
  Description automatically generated
* If the result is 1, the server is using **Windows Authentication mode** only.
* If the result is 0, the server is using **Mixed Mode Authentication**
* 
* Windows Authentication is the best practice for secure and centralized management, especially in modern domain-integrated environments. Mixed Mode can be used in hybrid scenarios but requires strict safeguards to mitigate potential risks.
* so auth mode supposes to be 1

**10. SQL Server Updates:**

* There are pending updates that need to be applied.
* A screenshot of a computer

  Description automatically generated

**11. RDP Access:**

* Only Domain admins have access to RDP
* 

**Recommendations:**

* **Update SQL Server**: Upgrade to the latest compatible version to benefit from improved features and security patches.
* **Disable internet access** to reduce potential security risks.
* **Disable SA Account**: Deactivate the SA account to minimize the attack surface. Create and use a separate user account with specific permissions for administrative tasks.
* **Secure SA Password**: If disabling the SA account is not immediately possible, store its credentials securely in a credential manager like KeePass or 1Password and delete any plain-text storage files.
* **Refine Firewall Rules**: Limit services and access to the SQL server to only essential systems and users.
* **Apply Server Hardening**: Restrict drag-and-drop, copy-paste, and internet access. Strengthen the overall server security posture.
* **Authentication Settings**: Enforce Windows Authentication and disable Mixed Mode Authentication unless absolutely necessary.
* **Conduct Regular Assessments**: Continue performing vulnerability assessments and act on the findings promptly.