Cyber Shujaa

Cloud Security Specialist

Assignment 17 - Lab 5: Securing Azure SQL Database

NAME: WELDON KIPKIRUI KENEI

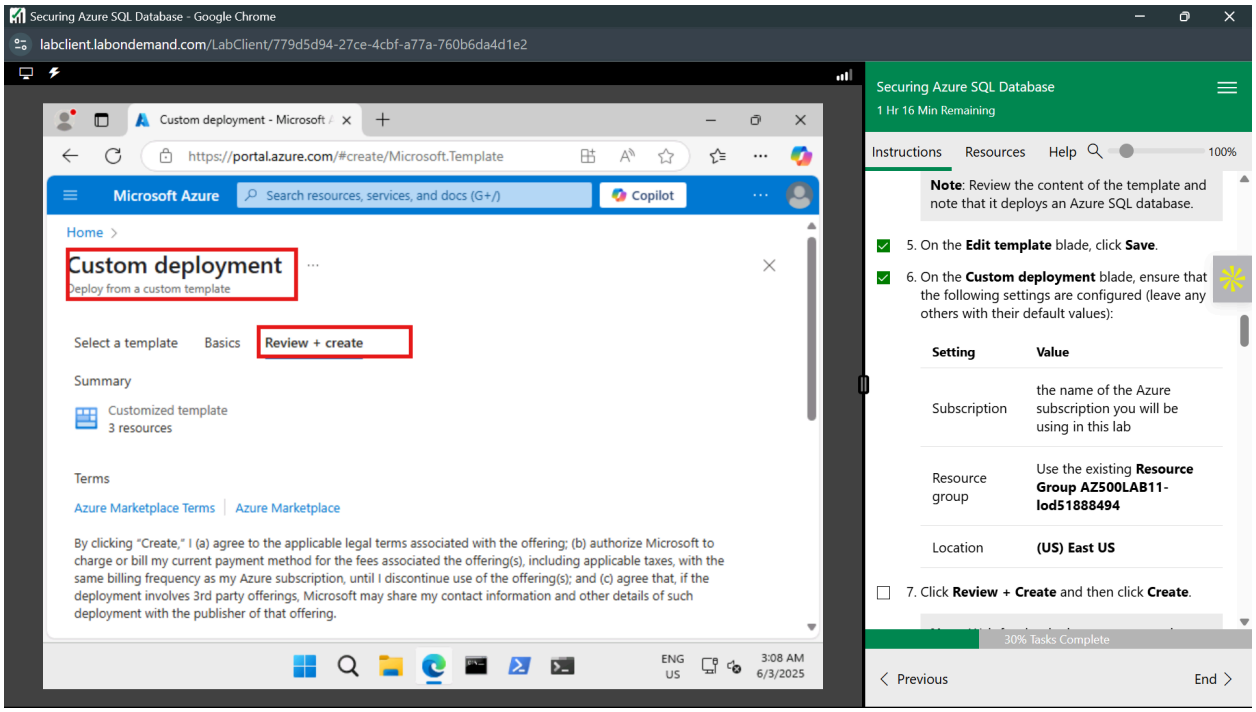
CS NO: ADC-CSS02-25027

Introduction

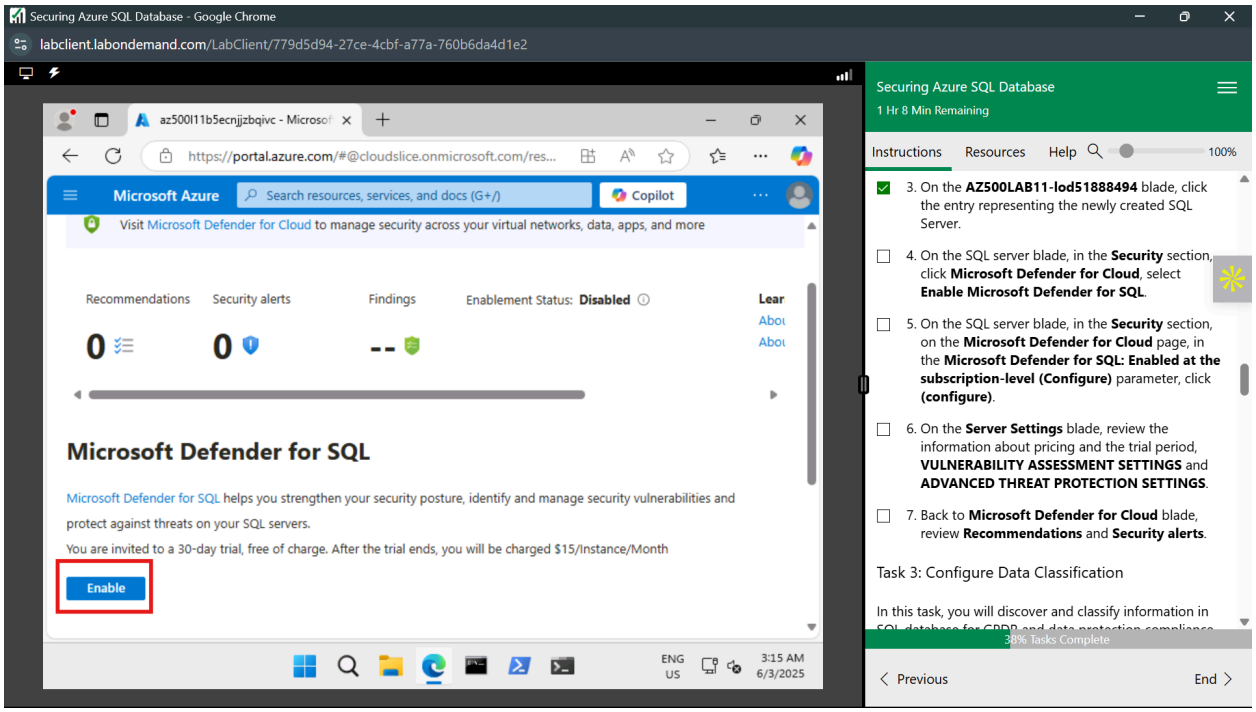
In this lab scenario, we have been tasked with reviewing the security features for the Azure SQL database. Specifically, we are interested in protecting against attacks such as SQL injection and data exfiltration. The ability to discover and classify database information, such as Confidential, and the ability to audit database server and database queries, and log events.

Implementing SQL Database security features

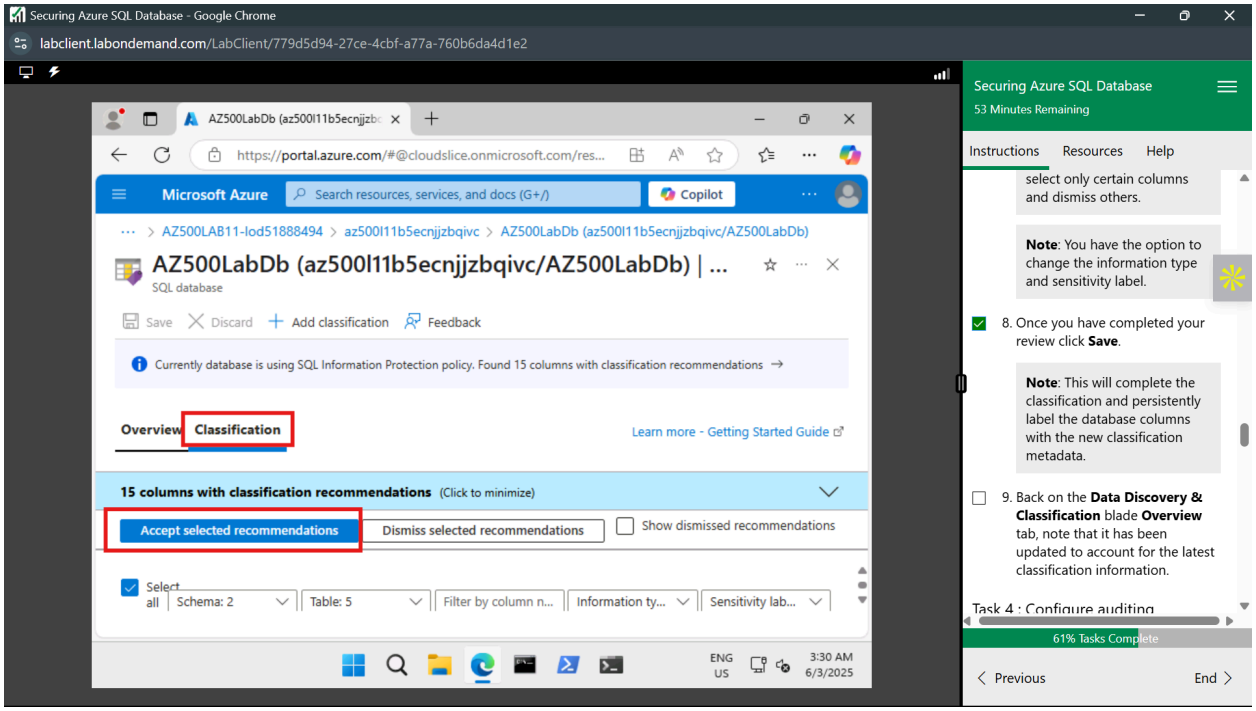
In this task, we will: Deploy an Azure SQL Database, configure Advanced Data Protection, configure Data Classification, and configure Auditing.
We deploy an Azure SQL database using a template as shown.



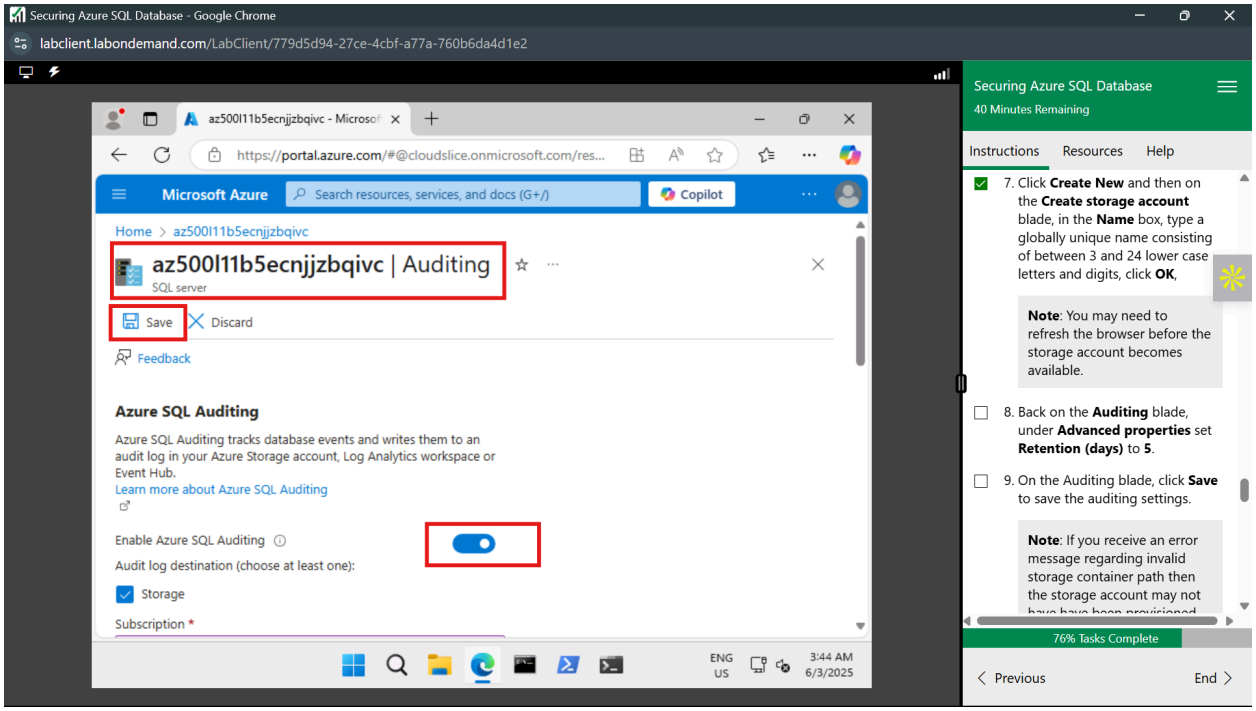
After the database is set, we then configure advanced data protections in the portal. This will be done by enabling Microsoft Defender for SQL.



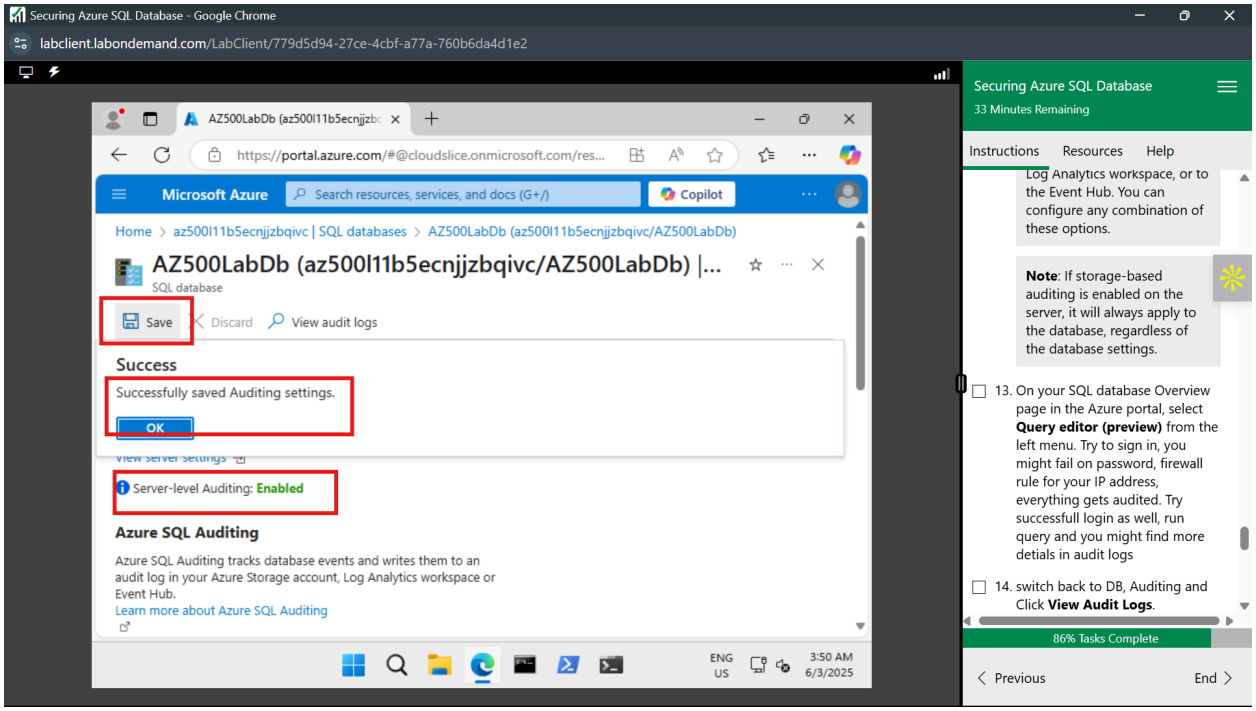
Next, we will discover and classify information in the SQL database for GDPR and data protection compliance.



Next, we will first configure server-level auditing and then configure database-level auditing. Shown below is server-level auditing. The default auditing settings include all the queries and stored procedures executed against the database, as well as successful and failed logins.



Since we already have the server-level auditing, we can configure the database-level auditing.



We can view the unified audit logs from the audit page for both server-level and database-level.

Conclusion

To conclude, the lab has equipped us with the ability to configure advanced secure data protection from the Azure portal for Azure SQL, identify and classify sensitive information in our database, and finally, how to audit our database and database servers through stored logs.