Azure Data Security – Protecting Your Environment

Tim Radney
tim@timradney.com

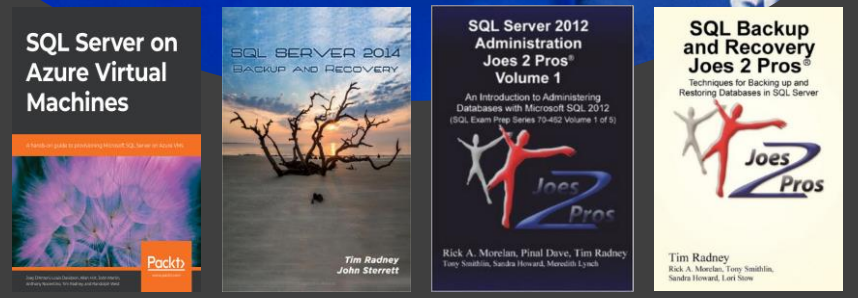
Speaker: Tim Radney

- Consultant/Trainer/Speaker/Author
- SaaS Migration Lead / Principal Consultant
- Email: **Tim@SQLskills.com and Tim@timradney.com**
- Blog: **https://www.SQLskills.com/blogs/Tim**
- Blog: **http://www.timradney.com**
- Microsoft Data Platform MVP
- Chapter Leader "Cloud Data Platform Virtual Group"

Key technology areas:

- Azure SQL Virtual Machine and storage
- SQL Server performance, tuning and optimization
- Azure Data Services Security
- Disaster Recovery
- Azure SQL DB / Managed Instance

@TRADNEY



Azure Data Security

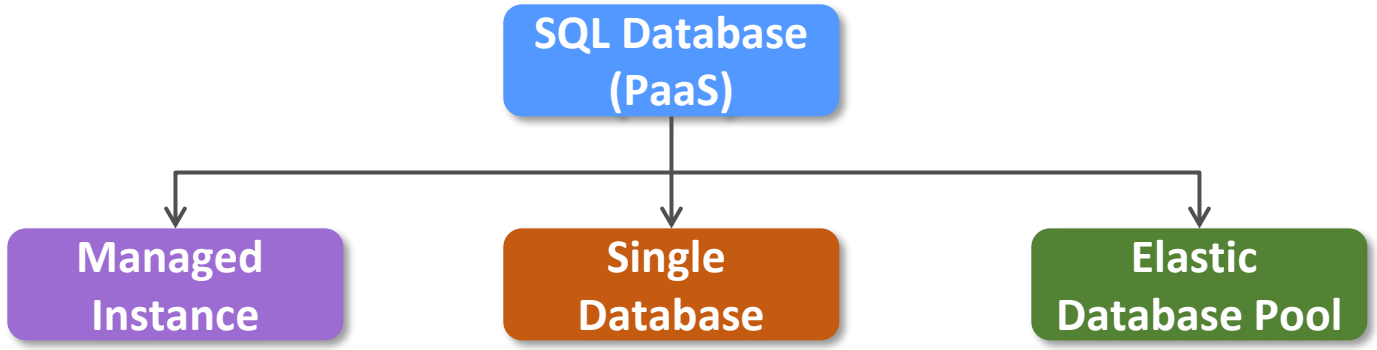
- What is Azure Platform as a Service
- Compliance
- Backups
- Privacy and Data Protection
- Threat and Vulnerability Protection
- Security Features
- Demo

What is Platform as a Service?

- Azure Cloud Services
  - Allows you to focus on applications, not hardware
  - Support for full lifecycle: building, testing, deploying, managing, updating
  - Auto-scale to meet demand and save money
  - Integrated health, monitoring, and load balancing
  - Predictable performance and pricing, pay-as-you-go
  - Secure and compliant for your sensitive data
  - Supports geographically distributed development teams
  - Pre-coded application components built-in: workflow, directory services, security, search, and more

Scalability and Reliability

- How does SQL Server fit into PaaS?
  - Azure SQL Database, Elastic Pools, and Managed Instance are built on Microsoft's Platform as a Service
  - Each product gets to take advantage of PaaS services and benefits



Compliance

- Many certifications
  - DoD Provisional Authorizations at Impact Levels 5, 4, and 2
  - FIPS 140-2 – US Federal Info Processing Standards
  - HIPPA/HITECH – Health Care
  - ISO 22301, 27001, 27017, 27018
  - PCI DSS – Payment Card industry
  - CJIS – US Criminal Justice Information Services
  - EU Model Clauses
  - And more..
- Microsoft compliance offerings: http://bit.ly/2lKjwzK

Backups

- Automated Backups - They are handled for you; you handle restores
  - Point-in-time restores
  - Retention is based on tier:
    - Basic = 7 days; Standard, Premium, Managed Instance = 35 days*
  - Restores are to a new database
    - https://azure.microsoft.com/en-us/documentation/articles/sql-database-business-continuity/
  - Backups are secure
  - Monitor backup storage costs for Azure SQL databases and elastic pools
  - Backup storage metrics are generally available (GA)

Privacy and Data Protection

- Dynamic Data Masking
  - Can limit access to sensitive data by controlling how the data appears
  - Masking rules can be defined on particular columns
  - No physical changes are made to the data
    - https://azure.microsoft.com/en-us/documentation/articles/sql-database-dynamic-data-masking-get-started/
- Row-Level Security
  - Can restrict row-level access based on a user's identity
  - Access restriction logic is located in the database tier
    - https://msdn.microsoft.com/en-us/library/dn765131.aspx

Privacy and Data Protection

- Transparent Data Encryption
  - Real-time encryption and decryption of the database, backups, and transaction log files at rest
  - Encrypts the storage of an entire database by using a symmetric key
  - On by default for new databases for Azure SQL DB and Managed Instance.
  - Manually enable for on-premises
  - Can Bring Your Own Key (BYOK) now
    - https://msdn.microsoft.com/en-us/library/dn948096.aspx

Privacy and Data Protection

- Always Encrypted
  - Allows clients to encrypt sensitive data inside client applications and not reveal the encryption keys to the Database Engine
  - Can ensure sensitive data never appears as plaintext inside the system
  - Only client applications or app servers that have access to the keys can access plaintext data
  - Encryption keys are stored in the Azure Key Vault
  - https://msdn.microsoft.com/en-us/library/mt163865.aspx

Always Encrypted – Types of Encryption

- **Randomized** – uses a method that encrypts data in a less predictable manner
- **Deterministic** – uses a method which always generates the same encrypted value for any given plaintext value

Randomized Encryption

Encrypt('123-45-6789') = 0x17cfd50a
Repeat: Encrypt('123-45-6789') = 0x9b1fcf32
Allows for transparent retrieval of encrypted data but NO operations
More secure

Deterministic Encryption

Encrypt('123-45-6789') = 0x85a55d3f
Repeat: Encrypt('123-45-6789') = 0x85a55d3f
Allows for transparent retrieval of encrypted data AND equality comparison
(i.e. in WHERE clauses and Joins, DISTINCT, GROUP BY)

Privacy and Data Protection

- Data Discovery and Classification
  - Detects potential sensitive data so you can tag it by classification
  - Part of the SQL Advanced Threat Protection (ATP) offering
  - Provides;
    - Discovery and recommendations
      - Scans your database and identifies columns containing potentially sensitive data
    - Labeling
      - Sensitivity classification labels can be persistently tagged on columns using new classification metadata attributes introduced into the SQL Engine. This can then be used for auditing
    - Query result set sensitivity
      - Sensitivity of query result set is calculated in real time for auditing purposes
    - Visibility
      - The database classification state can be viewed in the portal dashboard as well as download reports in Excel format for compliance and auditing needs

Threat/Vulnerability Protection

- Threat Detection
  - Allows customers to detect and respond to potential threats as they occur
  - Users receive alerts based upon suspicious activities, vulnerabilities, and more
  - Recommendations provided to help investigate and mitigate the threat
- Vulnerability Assessment
  - Service that provides visibility into your security state
  - Provides steps to investigate, manage, and resolve vulnerabilities
  - The tool uses a knowledge base of rules that flag security vulnerabilities and deviations from known best practices

Security Features

- Azure Active Directory integration
  - Allows you to centrally manage identities of database users and other Microsoft services
  - Azure Active Directory supports multi-factor authentication
- Managed Instance Auditing
  - Tracks database events and writes them to an audit log in your Azure storage account
  - Helps maintain regulatory compliance, gain insight into discrepancies, and understand database activity
- Data encryption in motion
  - Uses Transport Layer Security to encrypt data in motion

Demo:
Security Features

Row Level Security, Dynamic Data Masking, Always Encrypted


Thank You!
@tradney
tim@timradney.com