


**SQLskills *presenting* for
QCPASS SQL Server User Group
11th March 2020**

**Azure Data Security – Protecting Your
Environment**

Tim Radney
Tim@SQLskills.com



- Team of world-renowned SQL Server experts:
 - Paul S. Randal (@PaulRandal)
 - Kimberly L. Tripp (@KimberlyLTripp)
 - Jonathan Kehayias (@SQLPoolBoy)
 - Erin Stellato (@ErinStellato)
 - Tim Radney (@TRadney)
- Instructor-led training: Immersion Events
- Online training:  PLURALSIGHT <http://pluralsight.com/>
- Consulting: health checks, hardware, performance, upgrades
- Remote DBA: system monitoring and troubleshooting
- Conferences: PASS Summit, SQLintersection
- Become a SQLskills Insider
 - <http://www.sqlskills.com/Insider>



2020 Classes and Services

- 2020 Chicago (April - May) - ??
 - IEAzure: Immersion Event on Azure SQL DB, Managed Instance, and Azure VMs
 - IEReporting: Immersion Event on Using and Administering SSRS and PowerBI
 - IEPTO1: Immersion Event on Performance Tuning – Parts 1
 - IEPTO2: Immersion Event on Performance Tuning – Parts 2
 - IECAG: Immersion Event on Clustering and Availability Groups
- Online, live Immersion Events through the year
 - Always announced first with a discount in our newsletter (<https://www.sqlskills.com/Insider>)
- In-depth, instructor-led, technical training for SQL Server
- For more information: <https://www.sqlskills.com/training/>

- New client discount: US\$2,995 flat rate on first single-instance health check
- For more information: <https://www.sqlskills.com/services/>

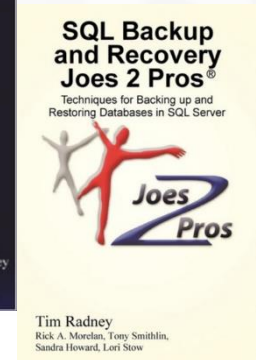
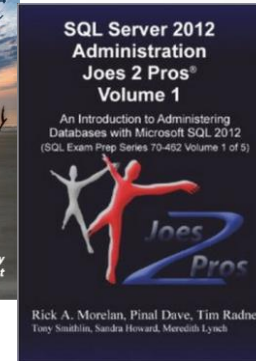
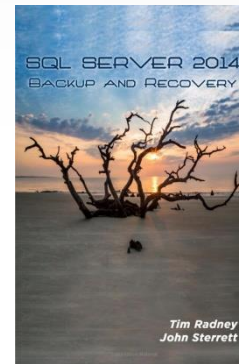
pluralsight

- Email paul@SQLskills.com with the subject line: **User Group Pluralsight code** to get a FREE (no catches, no credit card) 30-day trial of our 188+ hours of SQLskills content on Pluralsight
- For example:
 - <https://app.pluralsight.com/library/courses/sqlserver-logging/table-of-contents>
 - 7 hours on logging, recovery, and the transaction log (Paul)
 - <https://app.pluralsight.com/library/courses/sqlserver-indexing-for-performance>
 - 7 hours on indexing (Kimberly)
 - <https://www.pluralsight.com/courses/sqlserver-understanding-using-azure-sql-database>
 - 2 hours on Azure SQL Database (Tim)

Author/Instructor: Tim Radney



- Consultant/Trainer/Speaker/Author
- Principal Consultant, SQLskills.com
 - Email: Tim@SQLskills.com
 - Blog: <https://www.SQLskills.com/blogs/Tim>
 - Blog: <http://www.timradney.com>
 - Twitter: @TRadney
- Microsoft Data Platform MVP
- Chapter Leader "Columbus GA SQL Users Group"
- PASS Regional Mentor "South East USA"
- Outstanding PASS Volunteer
- Regular presenter at worldwide conferences on administration, disaster recovery, performance tuning, and Azure
- Friend of Red Gate
- (I also like electronics, aquaponics, farming chickens, crops, and tilapia)



SQL
intersection

Overview

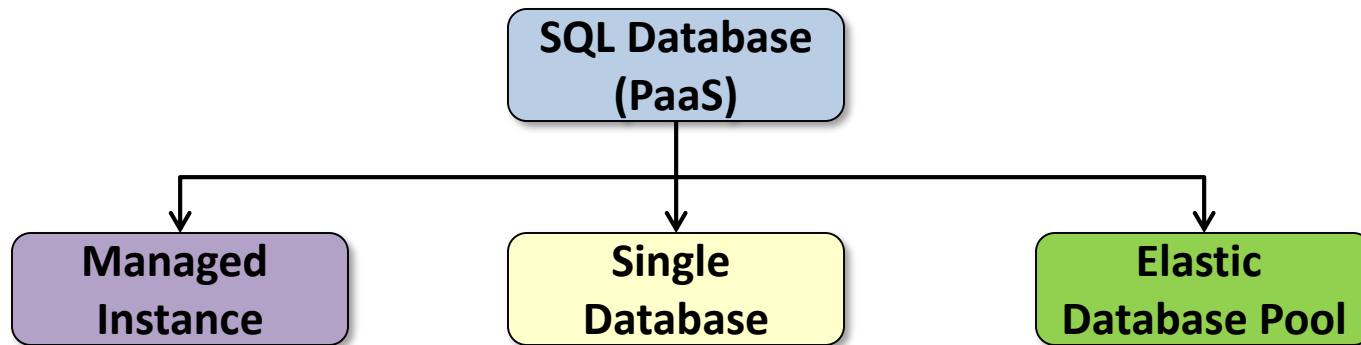
- What is Azure Platform as a Service?
- Compliance
- Backups
- Privacy and Data Protection
- Threat and Vulnerability Protection
- Security Features
- Demo

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

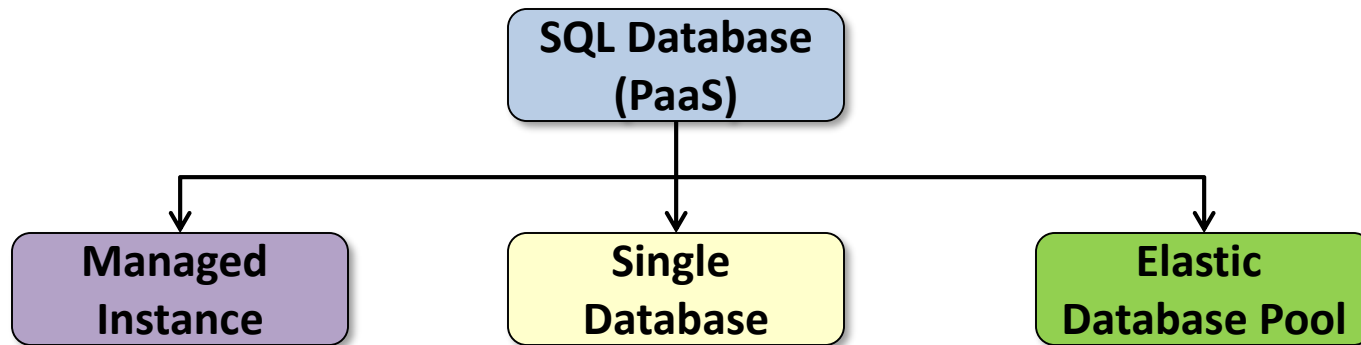
Platform as a Service

- 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



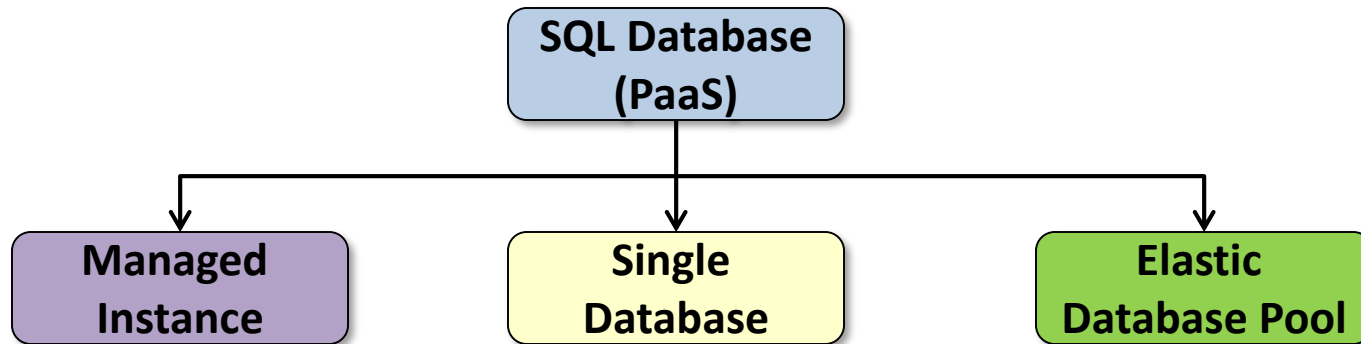
Platform as a Service

- 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



Platform as a Service

- 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
- Azure Trust Center <http://bit.ly/2lKjwzK>

Backups

- Automated Backups
 - Azure SQL Database, Elastic database, and Managed Instance all have backups happening behind the scenes
 - You are responsible for restoring and can restore to a point in time during your retention period
 - You don't have access to the backup files, these are protected within the Azure Fabric

Privacy/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/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 in Azure SQL DB, manually enable for on-premises and MI
 - Can Bring Your Own Key (BYOK) now
 - <https://msdn.microsoft.com/en-us/library/dn948096.aspx>
- 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/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

DEMOS



Summary

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

Thank you!

@tradney

tim@sqlskills.com

