Microsoft SQL Server v cloudu

RNDr. David Gešvindr
MVP: Data Platform | MCSE: Data Platform | MCT
david@wug.cz
@gesvindr

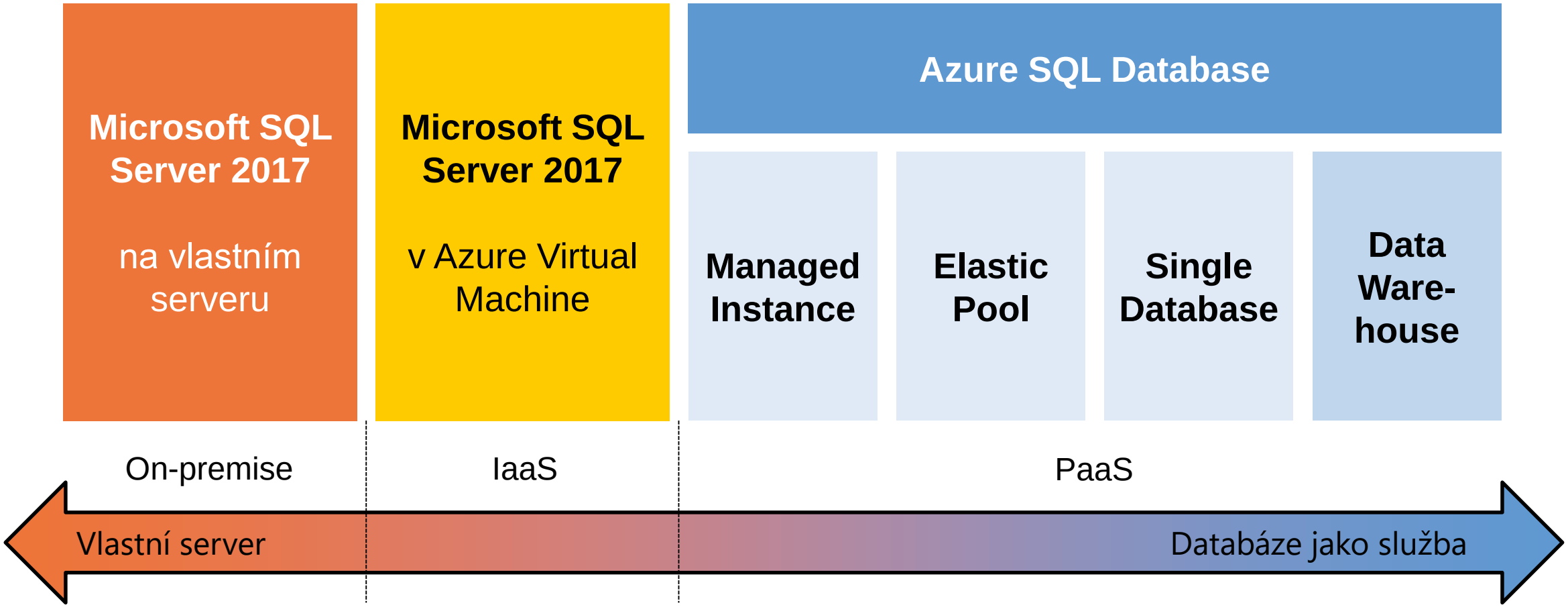
Osnova

1. Představení služby Azure SQL Database
2. Varianta Single Database
3. Varianta Elastic Pool
4. Varianta Managed Instance
5. Další služby Azure SQL Database

Osnova

1. **Představení služby Azure SQL Database**
2. Varianta Single Database
3. Varianta Elastic Pool
4. Varianta Managed Instance
5. Další služby Azure SQL Database

Možnosti provozu SQL Server databáze



Azure SQL Database

- **Relační databáze hostovaná jako služba v Microsoft Azure**
- Kompatibilní s Microsoft SQL Serverem
  - Stejné datové typy
  - T-SQL
  - Aplikační protokol TDS, TCP/IP 1433
  - Klienti
- Microsoft vyvíjí SQL Server a Azure SQL Database v jedné vývojové větvi

Klíčové vlastnosti

- **Vysoká dostupnost**
  - Dle SLA **99,99% dostupnost databáze** (4 minuty výpadek za měsíc)
  - Automatická synchronní replikace databáze na 3 servery
  - Je možné mít read-only repliku i v jiném data centru

- Za infrastrukturu zodpovídá Microsoft
  - Updaty serverů + OS
  - Zabezpečení, zálohy a integrita databáze

- **Neřešíte licence** – platíte za výkon, nikoliv za počet klientů

Varianty služby

- **Single Database**
  - Vhodná pro hosting izolovaných databází s vyrovnanou zátěží u aplikací navrhovaných pro cloud
- **Elastic Pool**
  - Vhodná pro hosting skupiny izolovaných databází s nevyrovnanou zátěží (SaaS aplikace, zákazníci izolováni na úrovni DB)
- **Managed Instance**
  - Jednoduchá migrace databází z IaaS do PaaS prostředí
  - Instance SQL Serveru s výhodami PaaS prostředí

Osnova

1. Představení služby Azure SQL Database
2. **Varianta Single Database**
3. Varianta Elastic Pool
4. Varianta Managed Instance
5. Další služby Azure SQL Database

Azure SQL Database – Single Database

- Izolované databáze hostované v rámci logického serveru
- Logický server seskupuje databáze z pohledu správy
  - Správa loginů pro přihlášení k databázi, kde je login mapován na database user
  - Databáze na jednom logickém serveru jsou rozmístěny na různých fyzických serverech
- Každá databáze je účtována zvlášť, dle alokovaného výkonu
  - Nevýhodné, pokud jsou databáze vytížené jen krátkodobě – řešením je Elastic Pool

Omezení Single Database a Elastic Pool

- **Je to jen databáze, chybí:**
  - SQL Agent (náhradou je Azure Automation, Azure Functions nebo Azure WebJobs)
  - Integration Services (náhradou je Azure Data Factory)
  - Analysis Services (náhradou je Azure Analysis Services – pouze režim tabular)
  - Reporting Services (náhradou může být Power BI)

- **Nemáte přístup k instanci ve které databáze běží**
  - Správa databázových souborů
  - Cross-databázové dotazy, distribuované transakce
  - Systémové pohledy na úrovni instance
  - Serverové role

Problém sdíleného prostředí

- SQL Database je multi-tenant prostředí, kdy je databázový server sdílen více zákazníky

- První generace (edice Web a Business) používaly k přerozdělování výkonu mechanizmus **throttling**
  - „Až mě SQL Database nachytá, že škodím ostatním, odřízne mi spojení“

- Druhá generace (edice Basic, Standard a Premium v režimu DTU) využívají nový **Resource Governor**
  - „Jsou mi přiděleny dedikované zdroje na sdíleném stroji, nemohu škodit ostatním“

- Třetí generace (vCores) dedikují fyzické zdroje pro databázi

Database Transaction Unit (DTU)

- Jednotka abstrahující fyzické prostředky
- Popisuje relativní transakční propustnost v kombinaci CPU/paměť/disk

- Problém: *Vývojář nechce řešit výkon CPU, disků apod. databázového serveru, ale potřebuje zvolit dostatečný výkon databáze*

- Slouží k relativnímu porovnání výkonu jednotlivých edic
  - Standard 0 (10 DTU) má 2x větší transakční propustnost než Basic (5 DTU)

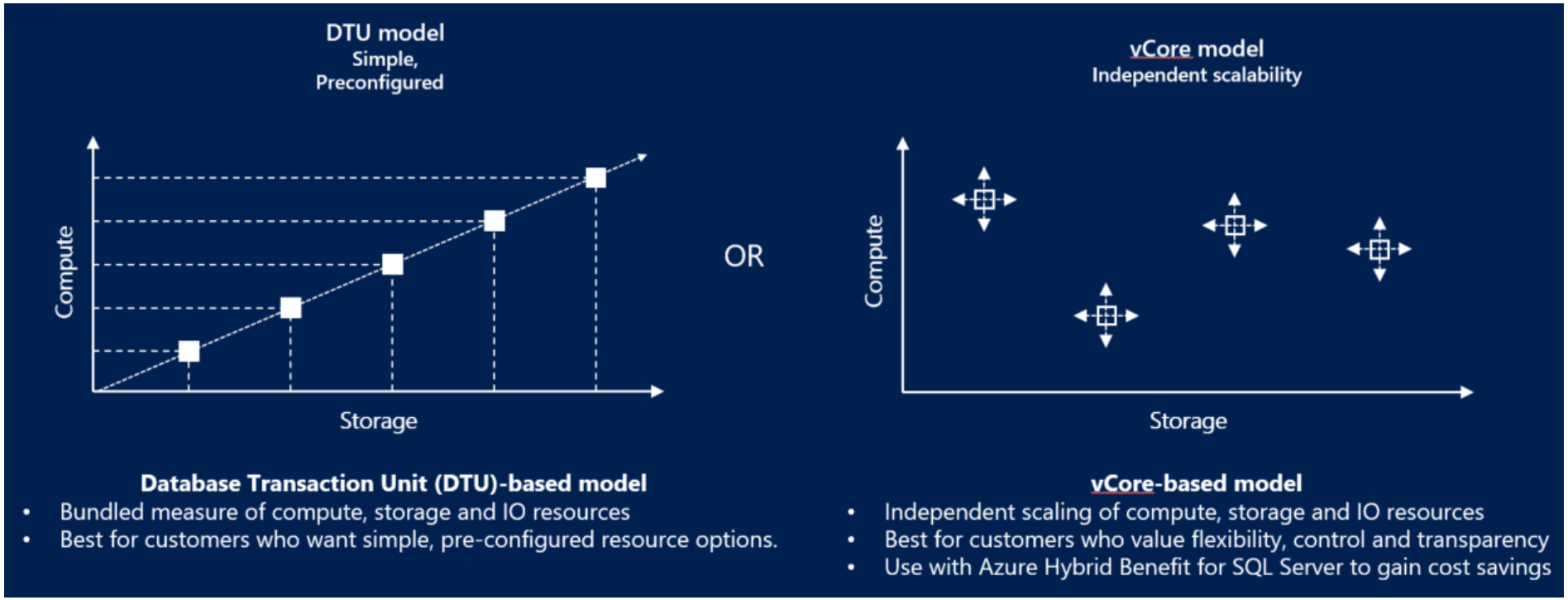
Service Tiers (DTU)

	Basic	Standard	Premium
Target workload	Development and production	Development and production	Development and production
Uptime SLA	99.99%	99.99%	99.99%
Backup retention	7 days	35 days	35 days
CPU	Low	Low, Medium, High	Medium, High
IO throughput (approximate)	2.5 IOPS per DTU	2.5 IOPS per DTU	48 IOPS per DTU
IO latency (approximate)	5 ms (read), 10 ms (write)	5 ms (read), 10 ms (write)	2 ms (read/write)
Columnstore indexing	N/A	S3 and above	Supported
In-memory OLTP	N/A	N/A	Supported

Zdroj: https://docs.microsoft.com/en-us/azure/sql-database/sql-database-service-tiers-dtu

vCore

- Pokud hledáte vyšší flexibilitu ohledně využití jednotlivých zdrojů (CPU, RAM, disk), můžete v preview vyzkoušet nákup výkonu po **„virtuálních jádrech“** nezávisle na úložišti



Zdroj: https://docs.microsoft.com/en-us/azure/sql-database/sql-database-service-tiers

Migrace databáze do cloudu

1. Vygenerovat T-SQL skript vytvářející schéma databáze a vkládající data s pomocí průvodce **Generate Scripts**

2. Použít průvodce **Deploy Database to Microsoft Azure SQL Database**

3. Vygenerovat BACPAC balíček (**Export Data-tier Application**), nahrát jej do Azure Storage a aktivovat import databáze

4. **Transakční replikace** – Azure SQL Database je možné nastavit jako push subscriber transakční replikace

Migrace databáze z cloudu

1. Exportovat databázi jako **BACPAC** balíček do Azure Storage
2. Volitelně stáhnout balíček na lokální server
3. S pomocí průvodce **Import Data-tier Application** jej nahrát na lokální SQL Server

Doporučená úprava aplikace

- **„Aplikace musí počítat s tím, že v cloudu může kdykoliv selhat cokoliv“**

- **Transient Error** – dočasný výpadek, přesměrování na jiný server

- Aplikace tyto typy chyb musí ošetřit a operaci zkusit znovu
  - Např.: Entity Framework Connection Resiliency and Retry Logic: https://msdn.microsoft.com/en-us/library/dn456835(v=vs.113).aspx
  - Implement resilient Entity Framework Core SQL connections: https://docs.microsoft.com/en-us/dotnet/standard/microservices-architecture/implement-resilient-applications/implement-resilient-entity-framework-core-sql-connections

Zabezpečení databáze

1. SQL Server Firewall
   - Nově s podporou virtuálních sítí, kdy je možné databázi zpřístupnit jen vašim službám v Azure nikoliv celému datacentru či vybraným adresám
2. Database Firewall
3. Autentizace
   - Podporováno SQL ověřování
   - Podporováno Azure AD ověřování včetně managed service identity
4. Autorizace
   - Aplikuje se bezpečnostní model SQL serveru v rámci databáze pro zpřístupnění zdrojů uživateli
   - Podpora pro **Row-level Security** a **Dynamic Data Masking**

Autentizace přes Azure Active Directory

- Na úrovni SQL Serveru je možné definovat **Active Directory admin** účet
  - Správce všech databází, ekvivalent SA vytvořeného spolu s SQL Serverem
  - Stejně vysoká práva, jako má vytvořený SA nejde přidělit jinému účtu

- Je podporováno i přihlašování uživatelů do databáze přes Azure AD

```
CREATE USER [david@wug.onmicrosoft.com] FROM EXTERNAL PROVIDER;
```

- Jsou podporovány i **Managed Service Identities**
  - Azure App Service aplikace se přihlašuje k databázi bez hesla: https://docs.microsoft.com/en-us/azure/app-service/app-service-web-tutorial-connect-msi

Šifrování dat

Při uložení

- **Transparent Database Encryption**
  - Celá databáze uložená v úložišti je zašifrována
  - Ochrana před odcizením databáze v datacentru
  - Microsoft automaticky generuje a spravuje šifrovací klíče
  - Nově je podporováno i použití vlastních klíčů uložených v Azure Key Vault
- **Always Encrypted**
  - Šifrovány vybrané sloupce na klientovi
  - Klíče nejsou uložené v databázi

Při přenosu

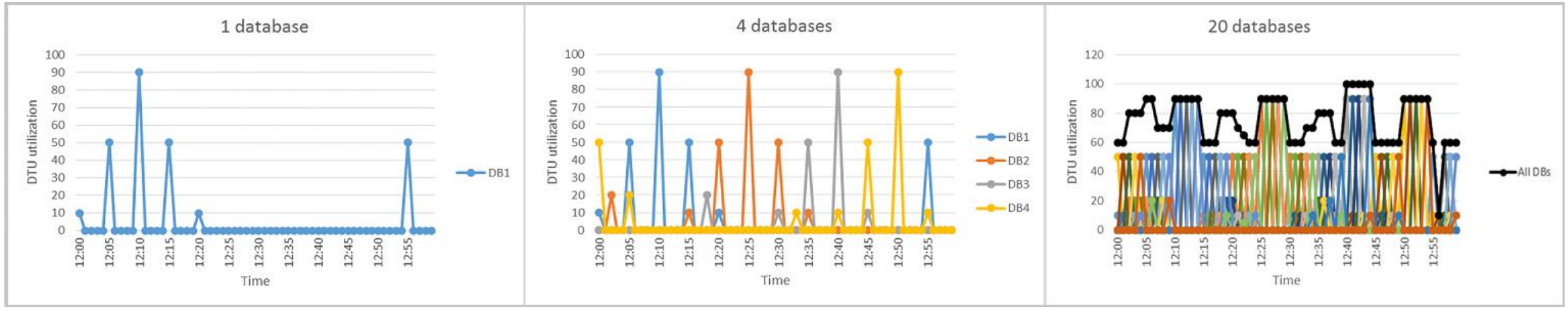
- **Encrypted Connection (TSL 1.2)**
  - Je vynuceno šifrování komunikace mezi klientem a databázovým serverem
  - Nešifrovaná spojení jsou blokována
  - Vaše aplikace by měla šifrování vynucovat, v případě ADO.NET:
    - Encrypt=True
    - TrustServerCertificate=False

Osnova

1. Představení služby Azure SQL Database
2. Varianta Single Database
3. **Varianta Elastic Pool**
4. Varianta Managed Instance
5. Další služby Azure SQL Database

Azure SQL Database – Elastic Pool

- Určeno pro hosting více databází, které sdílí výkon
  - Efektivnější využití alokovaného výkonu
- Zajímavé pro implementaci SaaS aplikací, kdy každý tenant (zákazník) může mít vlastní databázi



Zdroj: https://docs.microsoft.com/en-us/azure/sql-database/sql-database-elastic-pool

Omezení Elastic Pool

- Databáze sdílí výkon, ale pořád jsou izolované
  - Je možné nastavit rozpětí DTU pro databáze, aby se izoloval negativní dopad vytížených databází

- Není možné realizovat dotazy napříč databázemi a pracovat s instancí SQL Serveru
  - Stejná omezení jako u Single Database

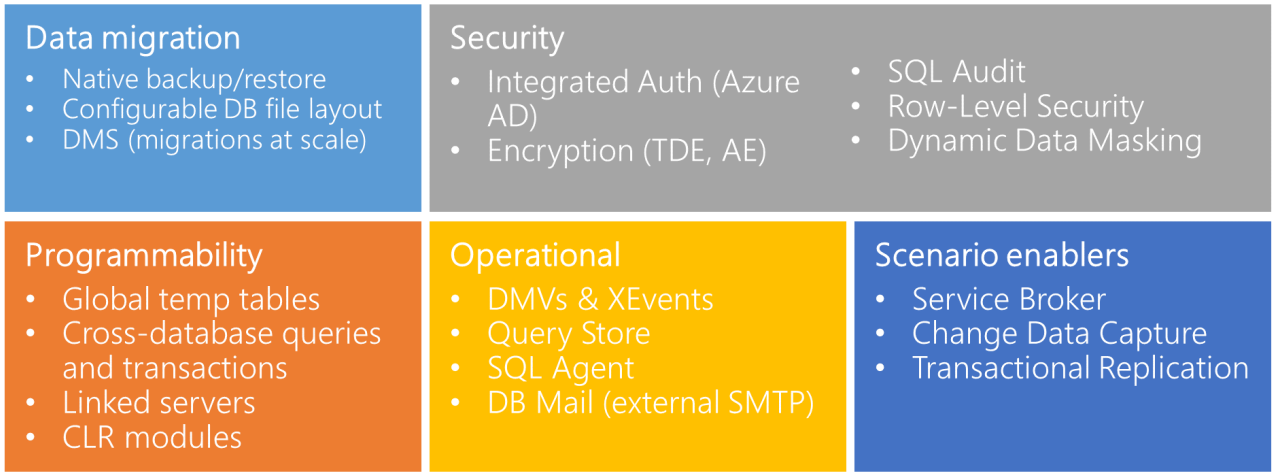
Osnova

1. Představení služby Azure SQL Database
2. Varianta Single Database
3. Varianta Elastic Pool
4. **Varianta Managed Instance**
5. Další služby Azure SQL Database

Azure SQL Database – Managed Instance

- Novinka **(preview)**, kdy je možné pronajmout celou instanci SQL Serveru **spravovanou Microsoftem**
- Řeší problémy s kompatibilitou současných aplikací při migraci do Azure SQL Database

Easy migration: nearly 100% like SQL Server



Note: Features will be added in stages until General Availability of Managed Instance.

Zdroj: https://docs.microsoft.com/en-gb/azure/sql-database/sql-database-managed-instance

PaaS výhody Managed Instances

- Nasazení a správa v režii Microsoftu
  - Nemáte přístup k OS, ale pouze k instanci SQL Serveru spravované Microsoftem
  - Velmi rychlé nasazení nové instance služby
  - Automatické aktualizace OS a SQL Serveru
- Automatické zálohy uložených databází
  - Možnost manuální copy only zálohy do Azure Storage
  - Možnost obnovy zálohy databáze z on-premise instance
  - Podpora Point-in-Time obnovy databáze ze zálohy

PaaS výhody Managed Instances

- Vysoká dostupnost **99,99%** dle SLA
  - Automatická synchronní replikace na 3 uzly v clusteru
  - Konfigurace AlwaysOn Availability Groups není přístupná – plně spravováno Microsoftem
- Izolované prostředí
  - Dedikované úložiště
  - Dedikované nesdílené výpočetní prostředky
  - Omezení síťového přístupu na konkrétní VNET

Odlišnosti od instance SQL Serveru

- Uživatelem aktivované zálohy musí být COPY ONLY
- Žádný příkaz **nesmí přistupovat na disky serveru**
  - BACKUP TO URL
  - BULK INSERT není podporován
  - Nový certifikát není možné založit načtením z disku
  - Při vytváření nových souborů databáze se nezadává cesta na disku – automaticky je každý soubor na novém disku
- Není možné měnit stav databáze a recovery model
- Linked servery jsou podporovány jen mezi SQL Servery

Odlišnosti od instance SQL Serveru

- SQL Server Agent podporuje jen kroky typu T-SQL
  - Není možné používat příkazovou řádku, SSIS a další typy kroků
- Database Mail funguje, aby jej mohl využít SQL Agent, musí být vytvořen profil AzureManagedInstance_dbmail_profile
- TempDB databáze má 12 souborů po 14 GB, maximální velikost je 168 GB

Osnova

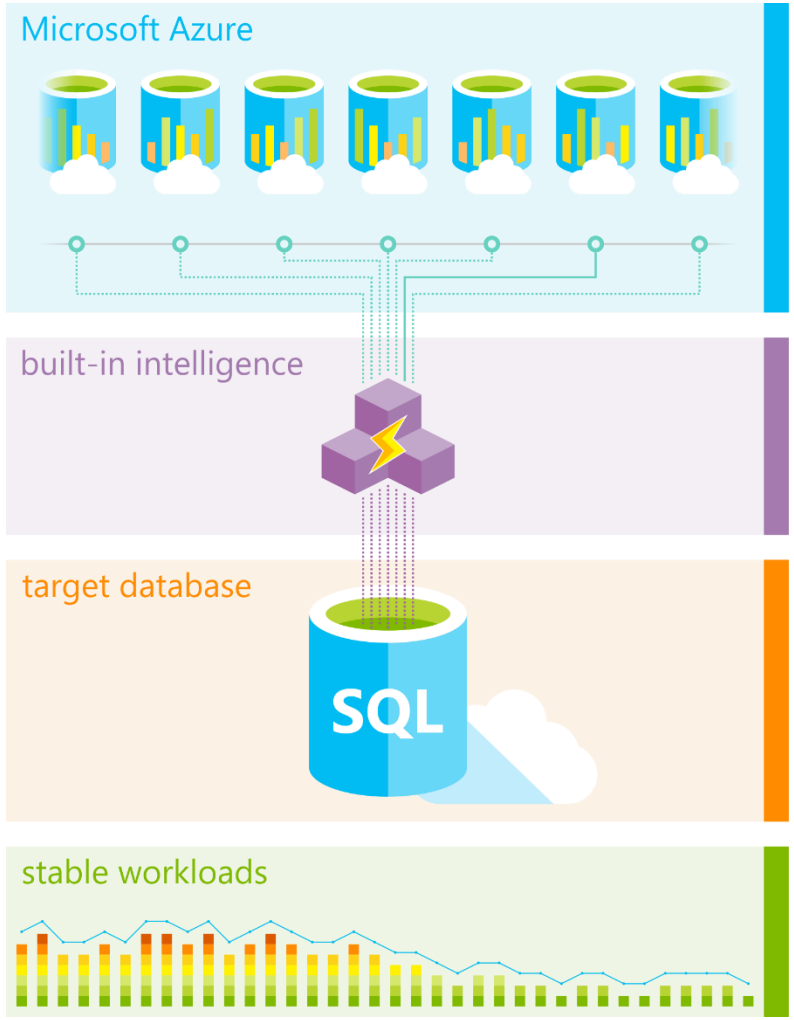
1. Představení služby Azure SQL Database
2. Varianta Single Database
3. Varianta Elastic Pool
4. Varianta Managed Instance
5. **Další služby Azure SQL Database**

Monitoring a správa databáze přes Azure portál

- Databázi je možné jednoduše monitorovat přes Azure portál a vybrané výkonnostní grafy složit do vlastního dashboardu

- Pokročilé funkce běžné konfigurovatelné v jazyce T-SQL můžeme jednoduše konfigurovat přes Azure portál

Automatic Database Tunning



horizontally learning
from all databases

finding optimization
opportunities

applying during
low-usage periods

verifying
performance gains
& reverting if required

Zdroj: https://docs.microsoft.com/en-us/azure/sql-database/sql-database-automatic-tuning

Threat Detection

- Detekce potenciálních útoků na hostované databáze
- Vyžaduje zapnutý SQL Audit
- Cena je 15$ za měsíc

- Umí detekovat např.:
  - Pokusy o SQL Injection
  - Netypická přihlášení

Azure SQL Database Data Discovery and Classification

- Sada nových funkcí, pro identifikaci a ochranu citlivých dat (GDPR)

1. Detekce potenciálně citlivých dat
2. Označení a klasifikace citlivosti dat
3. Výpočet citlivosti sady výsledků
4. Reporting

Osnova

1. Představení služby Azure SQL Database
2. Varianta Single Database
3. Varianta Elastic Pool
4. Varianta Managed Instance
5. Další služby Azure SQL Database

Související kurzy

Chcete si o Azure SQL Database nejen povídat 3 dny, ale také se s ní seznámit na praktických úkolech?

Můžete navštívit mé školení v Gopasu:

GOC 212 Microsoft Azure – Správa SQL Server relačních databází

GOPAS
POCITACOVA.SKOLA.CZ

Dotazy

RNDr. David Gešvindr
MVP: Data Platform | MCSE: Data Platform | MCT
david@wug.cz
@gesvindr