





SQL Managed Instance

Last updated by | Vitor Tomaz | Aug 5, 2020 at 12:45 PM PDT

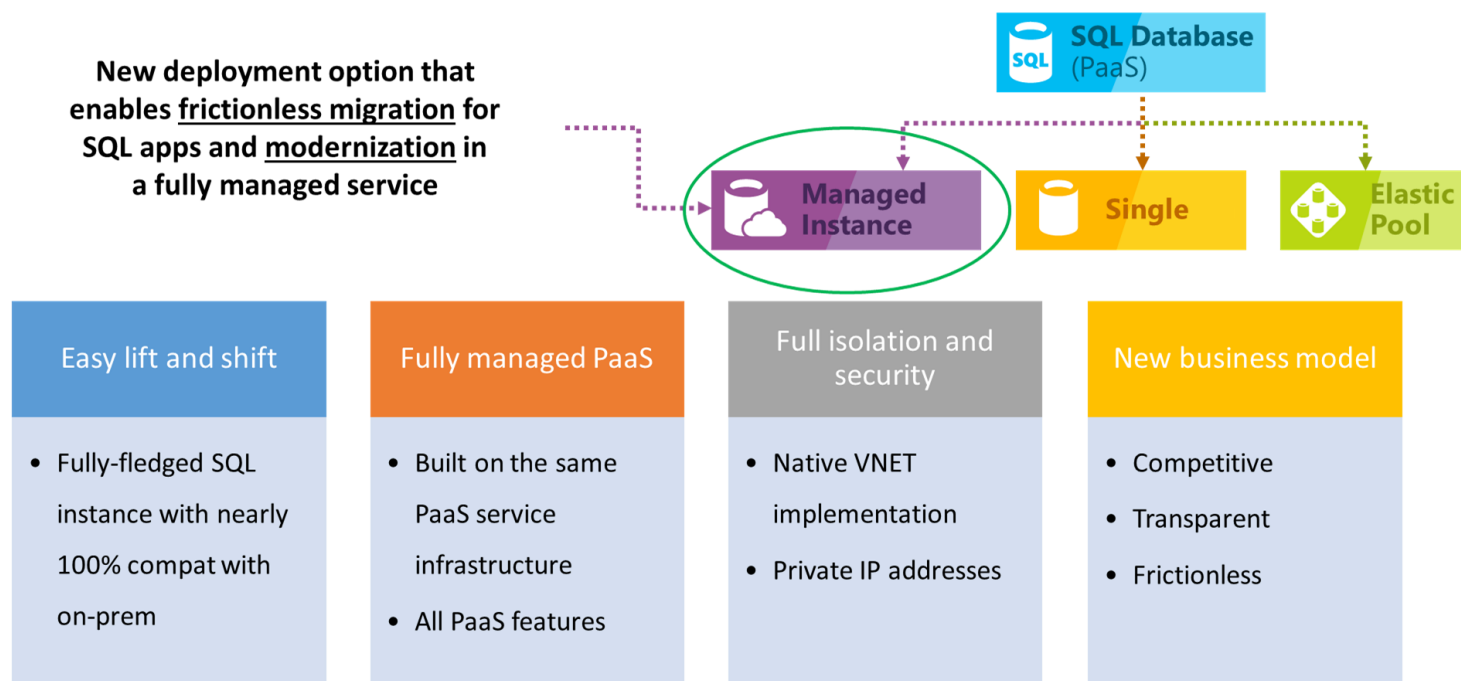
Contents

- [What is Azure SQL Database managed instance?](#)
 - [Key features and capabilities](#)
 - [vCore-based purchasing model](#)
 - [Managed instance service tiers](#)
 - [General purpose service tier](#)
 - [Business Critical service tier](#)
 - [Managed instance management operations](#)
 - [Instance availability during management](#)
 - [Canceling management operations](#)
 - [Advanced security and compliance](#)
 - [Managed instance security isolation](#)
 - [Azure SQL Database Security Features](#)
 - [Azure Active Directory Integration](#)
 - [Azure Active Directory integration and multi-factor authentication](#)
 - [Authentication](#)
 - [Authorization](#)
 - [Database migration](#)
 - [Back up and restore](#)
 - [Data Migration Service](#)
 - [SQL features supported](#)
 - [Key differences between SQL Server on-premises and in a ...](#)
 - [Managed instance administration features](#)
 - [How to programmatically identify a managed instance](#)
- [Next steps](#)

What is Azure SQL Database managed instance?

Managed instance is a new deployment option of Azure SQL Database, providing near 100% compatibility with the latest SQL Server on-premises (Enterprise Edition) Database Engine, providing a native [virtual network \(VNet\)](#)  implementation that addresses common security concerns, and a [business model](#)  favorable for on-premises SQL Server customers. The managed instance deployment model allows existing SQL Server customers to lift and shift their on-premises applications to the cloud with minimal application and database changes. At the same time, the managed instance deployment option preserves all PaaS capabilities (automatic patching and version updates, [automated backups](#) , [high-availability](#) ), that drastically reduces management overhead and TCO.

The following diagram outlines key features of managed instances:



The managed instance deployment model is designed for customers looking to migrate a large number of apps from on-premises or IaaS, self-built, or ISV provided environment to fully managed PaaS cloud environment, with as low migration effort as possible. Using the fully automated [Data Migration Service (DMS)] ([https://docs.microsoft.com/en-us/azure/dms/tutorial-sql-server-to-managed-instance#](https://docs.microsoft.com/en-us/azure/dms/tutorial-sql-server-to-managed-instance#%20create-an-azure-database-migration-service-instance) [create-an-azure-database-migration-service-instance](#)) in Azure, customers can lift and shift their on-premises SQL Server to a managed instance that offers compatibility with SQL Server on-premises and complete isolation of customer instances with native VNet support. With Software Assurance, you can exchange your existing licenses for discounted rates on a managed instance using the [Azure Hybrid Benefit for SQL Server](#) [.](#) A managed instance is the best migration destination in the cloud for SQL Server instances that require high security and a rich programmability surface.










The managed instance deployment option aims to deliver close to 100% surface area compatibility with the latest on-premises SQL Server version through a staged release plan.


To decide between the Azure SQL Database deployment options: single database, pooled database, and managed instance, and SQL Server hosted in virtual machine, see [how to choose the right version of SQL Server in Azure](#) [.](#)

Key features and capabilities



Managed instance combines the best features that are available both in Azure SQL Database and SQL Server Database Engine.

A managed instance runs with all of the features of the most recent version of SQL Server, including online operations, automatic plan corrections, and other enterprise performance enhancements. A Comparison of the features available is explained in [Feature comparison: Azure SQL Database versus SQL Server](#) [.](#)



PaaS benefits	Business continuity
<p>No hardware purchasing and management</p> <p>No management overhead for managing underlying infrastructure</p> <p>Quick provisioning and service scaling</p> <p>Automated patching and version upgrade</p> <p>Integration with other PaaS data services</p>	<p>99.99% uptime SLA</p> <p>Built in high-availability </p> <p>Data protected with automated backups </p> <p>Customer configurable backup retention period</p> <p>User-initiated backups </p> <p>[Point in time database restore]</p> <p>(https://docs.microsoft.com/azure/sql-database/sql-database-recovery-using-backups#  point-in-time-restore) capability</p>
Security and compliance	Management
<p>Isolated environment (VNet integration , single tenant service, dedicated compute and storage)</p> <p>Transparent data encryption (TDE) </p> <p>Azure AD authentication , single sign-on support</p> <p>Azure AD server principals (logins)</p> <p>Adheres to compliance standards same as Azure SQL database</p> <p>SQL auditing </p> <p>Advanced Threat Protection </p>	<p>Azure Resource Manager API for automating service provisioning and scaling</p> <p>Azure portal functionality for manual service provisioning and scaling</p> <p>Data Migration Service</p>

Azure SQL Database (all deployment options), has been certified against a number of compliance standards. For more information, see the [Microsoft Azure Trust Center](#)  where you can find the most current list of SQL Database compliance certifications.

The key features of managed instances are shown in the following table:


Feature	Description
SQL Server version / build	SQL Server Database Engine (latest stable)
Managed automated backups	Yes
Built-in instance and database monitoring and metrics	Yes
Automatic software patching	Yes
The latest Database Engine features	Yes
Number of data files (ROWS) per the database	Multiple
Number of log files (LOG) per database	1
VNet - Azure Resource Manager deployment	Yes
VNet - Classic deployment model	No
Portal support	Yes
Built-in Integration Service (SSIS)	No - SSIS is a part of Azure Data Factory PaaS 
Built-in Analysis Service (SSAS)	No - SSAS is separate PaaS 
Built-in Reporting Service (SSRS)	No - use Power BI or SSRS IaaS

vCore-based purchasing model

The [vCore-based purchasing model](#)  for managed instances gives you flexibility, control, transparency, and a straightforward way to translate on-premises workload requirements to the cloud. This model allows you to change compute, memory, and storage based upon your workload needs. The vCore model is also eligible for up to 55 percent savings with the [Azure Hybrid Benefit for SQL Server](#) .

In vCore model, you can choose between generations of hardware.

- **Gen4** Logical CPUs are based on Intel E5-2673 v3 (Haswell) 2.4-GHz processors, attached SSD, physical cores, 7-GB RAM per core, and compute sizes between 8 and 24 vCores.
- **Gen5** Logical CPUs are based on Intel E5-2673 v4 (Broadwell) 2.3-GHz and Intel SP-8160 (Skylake) processors, fast NVMe SSD, hyper-threaded logical core, and compute sizes between 4 and 80 cores.


Find more information about the difference between hardware generations in [managed instance resource limits](<https://docs.microsoft.com/azure/sql-database/sql-database-managed-instance-resource-limits#>  hardware-generation-characteristics).

New Gen4 databases are no longer supported in the Australia East or Brazil South regions.

Managed instance service tiers


Managed instance is available in two service tiers:



- **General purpose:** Designed for applications with typical performance and IO latency requirements.
- **Business critical:** Designed for applications with low IO latency requirements and minimal impact of underlying maintenance operations on the workload.


Both service tiers guarantee 99.99% availability and enable you to independently select storage size and compute capacity. For more information on the high availability architecture of Azure SQL Database, see [High availability and Azure SQL Database](#) .

General purpose service tier

The following list describes key characteristic of the General Purpose service tier:

- Design for the majority of business applications with typical performance requirements
- High-performance Azure Blob storage (8 TB)
- Built-in [high-availability](<https://docs.microsoft.com/azure/sql-database/sql-database-high-availability#basic-standard-and-general-purpose-service-tier-availability>) based on reliable Azure Blob storage and [Azure Service Fabric](#) .





For more information, see [storage layer in general purpose tier](#)  and [storage performance best practices and considerations for managed instances \(general purpose\)](#) .


Find more information about the difference between service tiers in [managed instance resource limits] (<https://docs.microsoft.com/azure/sql-database/sql-database-managed-instance-resource-limits#service-tier-characteristics>) .

Business Critical service tier

Business Critical service tier is built for applications with high IO requirements. It offers highest resilience to failures using several isolated replicas.

The following list outlines the key characteristics of the Business Critical service tier:

- Designed for business applications with highest performance and HA requirements
- Comes with super-fast local SSD storage (up to 1 TB on Gen4 and up to 4 TB on Gen5)
- Built-in [high availability](<https://docs.microsoft.com/azure/sql-database/sql-database-high-availability#premium-and-business-critical-service-tier-availability>) based on [Always On Availability Groups](#)  and [Azure Service Fabric](#) .
- Built-in additional [read-only database replica](#)  that can be used for reporting and other read-only workloads
- [In-Memory OLTP](#)  that can be used for workload with high-performance requirements

Find more information about the difference between service tiers in [managed instance resource limits] (<https://docs.microsoft.com/azure/sql-database/sql-database-managed-instance-resource-limits#service-tier-characteristics>) .

Managed instance management operations

Azure SQL Database provides management operations that you can use to automatically deploy new managed instances, update instance properties, and delete instances when no longer needed. This section provides information about management operations and their typical durations.

To support [deployments within Azure Virtual Networks (VNets)](<https://docs.microsoft.com/azure/virtual-network/virtual-network-for-azure-services#deploy-azure-services-into-virtual-networks>) and provide isolation and security for customers, managed instance relies on [virtual clusters] (<https://docs.microsoft.com/azure/sql-database/sql-database-managed-instance-connectivity-architecture#high-level-connectivity-architecture>), which represent a dedicated set of isolated virtual machines deployed inside the customer's virtual network subnet. Essentially, every managed instance deployment in an empty subnet results in a new virtual cluster buildout.

Subsequent operations on deployed managed instances might also have effects on its underlying virtual cluster. This affects the duration of management operations, as deploying additional virtual machines comes with an overhead that needs to be considered when you plan new deployments or updates to existing managed instances.

All management operations can be categorized as follows:

- Instance deployment (new instance creation).
- Instance update (changing instance properties, such as vCores or reserved storage).
- Instance deletion.

Typically, operations on virtual clusters take the longest. Duration of the operations on virtual clusters vary – below are the values that you can typically expect, based on existing service telemetry data:

- Virtual cluster creation. This is a synchronous step in instance management operations. **90% of operations finish in 4 hours.**
- Virtual cluster resizing (expansion or shrinking). Expansion is a synchronous step, while shrinking is performed asynchronously (without impact on the duration of instance management operations). **90% of cluster expansions finish in less than 2.5 hours.**
- Virtual cluster deletion. Deletion is an asynchronous step, but it can also be [initiated manually](#) on an empty virtual cluster, in which case it executes synchronously. **90% of virtual cluster deletions finish in 1.5 hours.**

Additionally, management of instances may also include one of the operations on hosted databases, which results in longer durations:

- Attaching database files from Azure Storage. This is a synchronous step, such as compute (vCore), or storage scaling up or down in the General Purpose service tier. **90% of these operations finish in 5 minutes.**
- Always On availability group seeding. This is a synchronous step, such as compute (vCore), or storage scaling in the Business Critical service tier as well as in changing the service tier from General Purpose to Business Critical (or vice versa). Duration of this operation is proportional to the total database size as well as current database activity (number of active transactions). Database activity when updating an instance can introduce significant variance to the total duration. **90% of these operations execute at 220 GB / hour or higher.**


The following table summarizes operations and typical overall durations:

Category	Operation	Long-running segment	Estimated duration
Deployment	First instance in an empty subnet	Virtual cluster creation	90% of operations finish in 4 hours
Deployment	First instance of another hardware generation in a non-empty subnet (for example, first Gen 5 instance in a subnet with Gen 4 instances)	Virtual cluster creation*	90% of operations finish in 4 hours
Deployment	First instance creation of 4 vCores, in an empty or non-empty subnet	Virtual cluster creation**	90% of operations finish in 4 hours
Deployment	Subsequent instance creation within the non-empty subnet (2nd, 3rd, etc. instance)	Virtual cluster resizing	90% of operations finish in 2.5 hours
Update	Instance property change (admin password, AAD login, Azure Hybrid Benefit flag)	N/A	Up to 1 minute
Update	Instance storage scaling up/down (General Purpose service tier)	Attaching database files	90% of operations finish in 5 minutes
Update	Instance storage scaling up/down (Business Critical service tier)	- Virtual cluster resizing - Always On availability group seeding	90% of operations finish in 2.5 hours + time to seed all databases (220 GB / hour)
Update	Instance compute (vCores) scaling up and down (General Purpose)	- Virtual cluster resizing - Attaching database files	90% of operations finish in 2.5 hours
Update	Instance compute (vCores) scaling up and down (Business Critical)	- Virtual cluster resizing - Always On availability group seeding	90% of operations finish in 2.5 hours + time to seed all databases (220 GB / hour)

Category	Operation	Long-running segment	Estimated duration
Update	Instance scale down to 4 vCores (General Purpose)	<ul style="list-style-type: none"> - Virtual cluster resizing (if done for the first time, it may require virtual cluster creation**) - Attaching database files 	90% of operations finish in 4 h 5 min**
Update	Instance scale down to 4 vCores (Business Critical)	<ul style="list-style-type: none"> - Virtual cluster resizing (if done for the first time, it may require virtual cluster creation**) - Always On availability group seeding 	90% of operations finish in 4 hours + time to seed all databases (220 GB / hour)
Update	Instance service tier change (General Purpose to Business Critical and vice versa)	<ul style="list-style-type: none"> - Virtual cluster resizing - Always On availability group seeding 	90% of operations finish in 2.5 hours + time to seed all databases (220 GB / hour)
Deletion	Instance deletion	Log tail backup for all databases	90% operations finish in up to 1 minute. Note: if last instance in the subnet is deleted, this operation will schedule virtual cluster deletion after 12 hours***
Deletion	Virtual cluster deletion (as user-initiated operation)	Virtual cluster deletion	90% of operations finish in up to 1.5 hours

* Virtual cluster is built per hardware generation.

** The 4 vCores deployment option was released in June 2019 and requires a new virtual cluster version. If you had instances in the target subnet that were all created before June 12, a new virtual cluster will be deployed automatically to host 4 vCore instances.

*** 12 hours is the current configuration but that might change in the future, so don't take a hard dependency on it. If you need to delete a virtual cluster earlier (to release the subnet for example), see [Delete a subnet after deleting an Azure SQL Database managed instance](https://supportability.visualstudio.com/AzureSQLDB/_wiki/wikis/AzureSQLDB.wiki/287388/SQL-Managed-Instance) .

Instance availability during management

Managed instances are not available to client applications during deployment and deletion operations.

Managed instances are available during update operations but there is a short downtime caused by the failover that happens at the end of updates that typically lasts up to 10 seconds. The exception to this is update of the reserved storage space in General Purpose service tier which does not incur failover nor affect instance availability.

Duration of a failover can vary significantly in case of long-running transactions that happen on the databases due to [prolonged recovery time](<https://docs.microsoft.com/azure/sql-database/sql-database-accelerated-database-recovery#the-current-database-recovery-process>). Hence it's not recommended to scale compute or storage of Azure SQL Database managed instance or to change service tier at the same time with the long-running transactions (data import, data processing jobs, index rebuild, etc.). Database failover that will be performed at the end of the operation will cancel ongoing transactions and result in prolonged recovery time.

Update of the reserved storage space in General Purpose service tier does not incur failover nor affect instance availability.

[Accelerated database recovery](#) is not currently available for Azure SQL Database managed instances. Once enabled, this feature will significantly reduce variability of failover time, even in case of long-running transactions.

Canceling management operations

The following table summarizes ability to cancel specific management operations and typical overall durations:

Category	Operation	Cancelable	Estimated cancel duration
Deployment	Instance creation	No	
Update	Instance storage scaling up/down (General Purpose)	No	
Update	Instance storage scaling up/down (Business Critical)	Yes	90% of operations finish in 5 minutes
Update	Instance compute (vCores) scaling up and down (General Purpose)	Yes	90% of operations finish in 5 minutes
Update	Instance compute (vCores) scaling up and down (Business Critical)	Yes	90% of operations finish in 5 minutes
Update	Instance service tier change (General Purpose to Business Critical and vice versa)	Yes	90% of operations finish in 5 minutes
Delete	Instance deletion	No	
Delete	Virtual cluster deletion (as user-initiated operation)	No	

In order to cancel the management operation, go to the overview blade and click on notification box of ongoing operation. From the right side, a screen with ongoing operation will appear and there will be button for canceling operation. After first click, you will be asked to click again and confirm that you want to cancel the operation.

Resource group (change) :

- Status : Updating
- Location : West Europe
- Subscription (change) :
- Subscription ID :

Tags (change) : [Click here to add tags](#)

Managed instance admin : urmila

Host :

Pricing tier : General Purpose Gen5 (256 GB, 4 vCores)

Instance pool : Not in an instance pool

Virtual network/subnet : MIVirtualNetwork/ManagedInstanceSubnet

Virtual cluster :

CPU utilization

1 hour 24 hours 7 days Aggregation type: Avg

Storage utilization

Current 1 GB
Quota 256 GB
0.5%

4 Managed Instance databases

Search to filter databases...

Name	Status
AdventureWorks2017	Online
AdventureWorks2017_restored	Online

Notifications (1) **Managed Instance features (1)**

All Alerts (0) Recommendations (0) Info (1)

You have 1 ongoing operation

This managed instance has some ongoing or recent operations. Click here to view them.

Ongoing operations
(SQL managed instance)

1 OPERATION

Updating managed instance

Update operation in progress...

Cancel this operation

](./media/sql-database-managed-instance/canceling-operation.png# lightbox)

After cancel request has been submitted and processed, you will get notification if cancel submission has been successful or not.

In case of cancel success, management operation will be canceled in couple of minutes resulting with a failure.

Notifications

[More events in the activity log →](#) [Dismiss all](#)

Failed to scale managed instance

Failed to scale the managed instance:
 ErrorCode: OperationCancelled
 ErrorMessage: The operation has been cancelled by user.

an hour ago

Successfully submitted managed instance operation cancellation...

Successfully submitted managed instance operation cancellation request for management operation on managed instance:

an hour ago

If cancel request fails or cancel button is not active, that means that management operation has entered not cancelable state and that it will finish in couple of minutes. Management operation will continue its execution until it is completed.

Canceling operation is currently supported only in Portal.

Advanced security and compliance

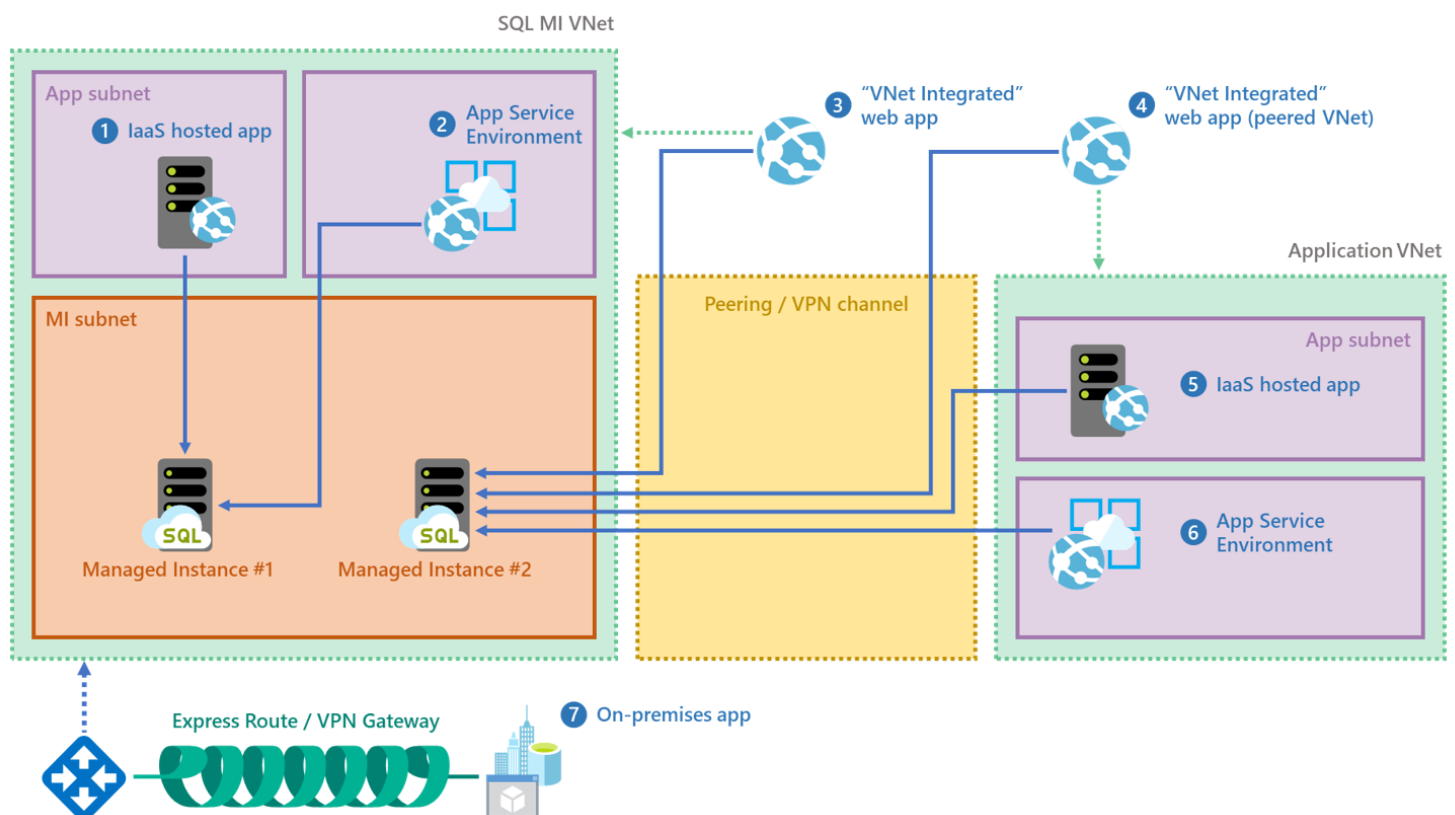
The managed instance deployment option combines advanced security features provided by Azure cloud and SQL Server Database Engine.

Managed instance security isolation

A managed instance provides additional security isolation from other tenants in the Azure cloud. Security isolation includes:

- [Native virtual network implementation](#) and connectivity to your on-premises environment using Azure Express Route or VPN Gateway.
- In a default deployment, SQL endpoint is exposed only through a private IP address, allowing safe connectivity from private Azure or hybrid networks.
- Single-tenant with dedicated underlying infrastructure (compute, storage).

The following diagram outlines various connectivity options for your applications:












To learn more details about VNet integration and networking policy enforcement at the subnet level, see [VNet architecture for managed instances](#) and [Connect your application to a managed instance](#).

Place multiple managed instance in the same subnet, wherever that is allowed by your security requirements, as that will bring you additional benefits. Collocating instances in the same subnet will significantly simplify networking infrastructure maintenance and reduce instance provisioning time, since long provisioning duration is associated with the cost of deploying the first managed instance in a subnet.

Azure SQL Database Security Features

Azure SQL Database provides a set of advanced security features that can be used to protect your data.

- [Managed instance auditing](#)  tracks database events and writes them to an audit log file placed in your Azure storage account. Auditing can help maintain regulatory compliance, understand database activity, and gain insight into discrepancies and anomalies that could indicate business concerns or suspected security violations.
- Data encryption in motion - a managed instance secures your data by providing encryption for data in motion using Transport Layer Security. In addition to transport layer security, the managed instance deployment option offers protection of sensitive data in flight, at rest and during query processing with [Always Encrypted](#) . Always Encrypted is an industry-first that offers unparalleled data security against breaches involving the theft of critical data. For example, with Always Encrypted, credit card numbers are stored encrypted in the database always, even during query processing, allowing decryption at the point of use by authorized staff or applications that need to process that data.
- [Advanced Threat Protection](#)  complements [auditing](#)  by providing an additional layer of security intelligence built into the service that detects unusual and potentially harmful attempts to access or exploit databases. You are alerted about suspicious activities, potential vulnerabilities, and SQL injection attacks, as well as anomalous database access patterns. Advanced Threat Protection alerts can be viewed from [Azure Security Center](#)  and provide details of suspicious activity and recommend action on how to investigate and mitigate the threat.
- [Dynamic data masking](#)  limits sensitive data exposure by masking it to non-privileged users. Dynamic data masking helps prevent unauthorized access to sensitive data by enabling you to designate how much of the sensitive data to reveal with minimal impact on the application layer. It's a policy-based security feature that hides the sensitive data in the result set of a query over designated database fields, while the data in the database is not changed.
- [Row-level security](#)  enables you to control access to rows in a database table based on the characteristics of the user executing a query (such as by group membership or execution context). Row-level security (RLS) simplifies the design and coding of security in your application. RLS enables you to implement restrictions on data row access. For example, ensuring that workers can access only the data rows that are pertinent to their department, or restricting a data access to only the relevant data.
- [Transparent data encryption \(TDE\)](#)  encrypts managed instance data files, known as encrypting data at rest. TDE performs real-time I/O encryption and decryption of the data and log files. The encryption uses a database encryption key (DEK), which is stored in the database boot record for availability during recovery. You can protect all your databases in a managed instance with transparent data encryption. TDE is SQL Server's proven encryption-at-rest technology that is required by many compliance standards to protect against theft of storage media.

Migration of an encrypted database to a managed instance is supported via the Azure Database Migration Service (DMS) or native restore. If you plan to migrate an encrypted database using native restore, migration of the existing TDE certificate from the SQL Server on-premises or SQL Server in a virtual machine to a managed instance is a required step. For more information about migration options, see [SQL Server instance migration to managed instance](#) .

Azure Active Directory Integration

The managed instance deployment option supports traditional SQL server Database engine logins and logins integrated with Azure Active Directory (AAD). Azure AD server principals (logins) (**public preview**) are Azure cloud version of on-premises database logins that you are using in your on-premises environment. Azure AD server principals (logins) enable you to specify users and groups from your Azure Active Directory tenant as true instance-scoped principals, capable of performing any instance-level operation, including cross-database queries within the same managed instance.

A new syntax is introduced to create Azure AD server principals (logins), **FROM EXTERNAL PROVIDER**. For more information on the syntax, see [CREATE LOGIN](https://docs.microsoft.com/azure/sql-database/sql-database-aad-authentication-configure#provision-an-azure-active-directory-administrator-for-your-managed-instance), and review the [Provision an Azure Active Directory administrator for your managed instance](<https://docs.microsoft.com/azure/sql-database/sql-database-aad-authentication-configure#provision-an-azure-active-directory-administrator-for-your-managed-instance>) article.

Azure Active Directory integration and multi-factor authentication

The managed instance deployment option enables you to centrally manage identities of database user and other Microsoft services with [Azure Active Directory integration](#). This capability simplified permission management and enhances security. Azure Active Directory supports [multi-factor authentication](#) (MFA) to increase data and application security while supporting a single sign-on process.

Authentication

Managed instance authentication refers to how users prove their identity when connecting to the database. SQL Database supports two types of authentication:

- **SQL Authentication:**

This authentication method uses a username and password.

- **Azure Active Directory Authentication:**

This authentication method uses identities managed by Azure Active Directory and is supported for managed and integrated domains. Use Active Directory authentication (integrated security) [whenever possible](#).

Authorization



Authorization refers to what a user can do within an Azure SQL Database, and is controlled by your user account's database role memberships and object-level permissions. A Managed instance has same authorization capabilities as SQL Server 2017.

Database migration

The managed instance deployment option targets user scenarios with mass database migration from on-premises or IaaS database implementations. Managed instance supports several database migration options:


Back up and restore

The migration approach leverages SQL backups to Azure Blob storage. Backups stored in Azure storage blob can be directly restored into a managed instance using the [T-SQL RESTORE command](#).



- For a quickstart showing how to restore the Wide World Importers - Standard database backup file, see [Restore a backup file to a managed instance](#) . This quickstart shows you have to upload a backup file to Azure blob storage and secure it using a Shared access signature (SAS) key.
- For information about restore from URL, see [Native RESTORE from URL] ([https://docs.microsoft.com/azure/sql-database/sql-database-managed-instance-migrate#](https://docs.microsoft.com/azure/sql-database/sql-database-managed-instance-migrate#native-restore-from-url)  native-restore-from-url).

Backups from a managed instance can only be restored to another managed instance. They cannot be restored to an on-premises SQL Server or to a single database/elastic pool.

Data Migration Service

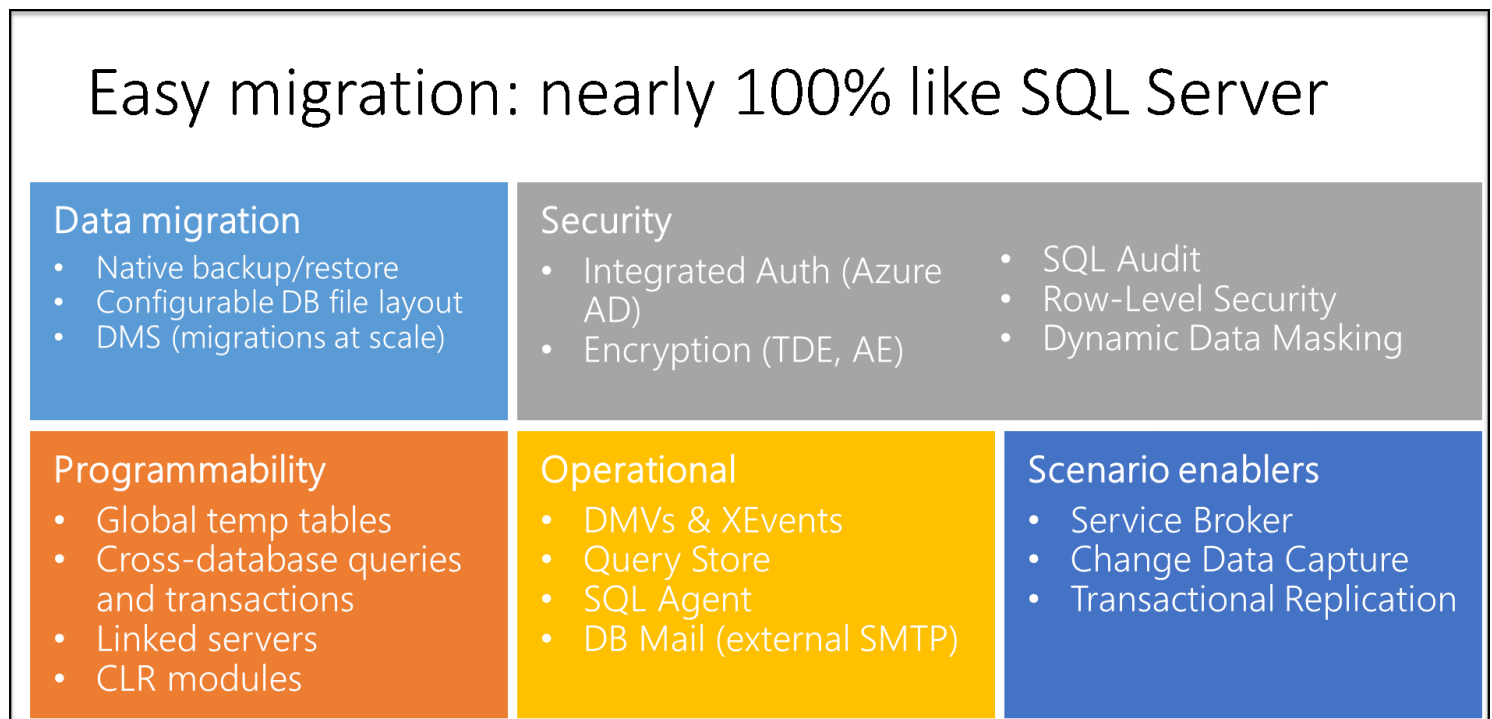
The Azure Database Migration Service is a fully managed service designed to enable seamless migrations from multiple database sources to Azure Data platforms with minimal downtime. This service streamlines the tasks required to move existing third party and SQL Server databases to Azure SQL Database (single databases, pooled databases in elastic pools, and instance databases in a managed instance) and SQL Server in Azure VM. See [How to migrate your on-premises database to managed instance using DMS](#) .

SQL features supported

The managed instance deployment option aims to deliver close to 100% surface area compatibility with on-premises SQL Server coming in stages until service general availability. For a features and comparison list, see [SQL Database feature comparison](#) , and for a list of T-SQL differences in managed instances versus SQL Server, see [managed instance T-SQL differences from SQL Server](#) .





The managed instance deployment option supports backward compatibility to SQL 2008 databases. Direct migration from SQL 2005 database servers is supported, compatibility level for migrated SQL 2005 databases are updated to SQL 2008.

The following diagram outlines surface area compatibility in managed instance:











Key differences between SQL Server on-premises and in a managed instance

The managed instance deployment option benefits from being always-up-to-date in the cloud, which means that some features in on-premises SQL Server may be either obsolete, retired, or have alternatives. There are specific cases when tools need to recognize that a particular feature works in a slightly different way or that the service is running in an environment you do not fully control:

- High-availability is built in and pre-configured using technology similar to [Always On Availability Groups](#) .
- Automated backups and point in time restore. Customer can initiate `copy-only` backups that do not interfere with automatic backup chain.
- Managed instance does not allow specifying full physical paths so all corresponding scenarios have to be supported differently: RESTORE DB does not support WITH MOVE, CREATE DB doesn't allow physical paths, BULK INSERT works with Azure Blobs only, etc.
- Managed instance supports [Azure AD authentication](#)  as cloud alternative to Windows authentication.
- Managed instance automatically manages XTP filegroup and files for databases containing In-Memory OLTP objects
- Managed instance supports SQL Server Integration Services (SSIS) and can host SSIS catalog (SSISDB) that stores SSIS packages, but they are executed on a managed Azure-SSIS Integration Runtime (IR) in Azure Data Factory (ADF), see [Create Azure-SSIS IR in ADF](#) . To compare the SSIS features in SQL Database, see [Compare an Azure SQL Database single database, elastic pool, and managed instance] (<https://docs.microsoft.com/azure/data-factory/create-azure-ssis-integration-runtime#>  [comparison-of-a-sql-database-single-database-elastic-pool-and-managed-instance](#)).

Managed instance administration features

The managed instance deployment option enables system administrator to spend less time on administrative tasks because the SQL Database service either performs them for you or greatly simplifies those tasks. For example, [OS / RDBMS installation and patching](#) , [dynamic instance resizing and configuration](#) , [backups](#) , [database replication](#)  (including system databases), [high availability configuration](#) , and configuration of health and [performance monitoring](#)  data streams.

For a list of supported, partially supported, and unsupported features, see [SQL Database features](#) . For a list of T-SQL differences in managed instances versus SQL Server, see [managed instance T-SQL differences from SQL Server](#) .

How to programmatically identify a managed instance

The following table shows several properties, accessible through Transact SQL, that you can use to detect that your application is working with managed instance and retrieve important properties.

Property	Value	Comment
@@VERSION	Microsoft SQL Azure (RTM) - 12.0.2000.8 2018-03-07 Copyright (C) 2018 Microsoft Corporation.	This value is same as in SQL Da not indicate SQL engine versio 2014). Managed instance always stable SQL engine version, which higher than latest available RTM Server.
SERVERPROPERTY ('Edition')	SQL Azure	This value is same as in SQL Da
SERVERPROPERTY('EngineEdition')	8	This value uniquely identifies a
@@SERVERNAME , SERVERPROPERTY ('ServerName')	Full instance DNS name in the following format: <instancename> . <dnsprefix> .database.windows.net, where <instancename> is name provided by the customer, while <dnsprefix> is autogenerated part of the name guaranteeing global DNS name uniqueness ("wcus17662feb9ce98", for example)	Example: my-managed-instance.wcus17662feb9ce98.d ☐

Next steps

- To learn how to create your first managed instance, see [Quickstart guide](#) ☐.
- For a features and comparison list, see [SQL common features](#) ☐.
- For more information about VNet configuration, see [managed instance VNet configuration](#) ☐.
- For a quickstart that creates a managed instance and restores a database from a backup file, see [create a managed instance](#) ☐.
- For a tutorial using the Azure Database Migration Service (DMS) for migration, see [managed instance migration using DMS](#) ☐.
- For advanced monitoring of managed instance database performance with built-in troubleshooting intelligence, see [Monitor Azure SQL Database using Azure SQL Analytics](#) ☐.
- For pricing information, see [SQL Database managed instance pricing](#) ☐. </dnsprefix> </instancename> </dnsprefix> </instancename>

How good have you found this content?

