Kickstart for SQL Server & SQL Database

In this article, we will go, step by step, to create SQL Server & Database on Microsoft Azure. Microsoft Azure SQL Database (formerly SQL Azure, SQL Server Data Services, SQL Services, Windows Azure SQL Database) is a cloud-based service from Microsoft, offering data-storage capabilities. The aim is for users to just communicate with a T-SQL endpoint rather than managing database storage, files, and high availability.

Current versions of Microsoft Azure SQL Database share a common code-base with Microsoft SQL Server. This database engine allows users to make relational queries against stored data which can either be structured or semi-structured, and unstructured documents.

SQL Database features include, querying data, search, data analysis, and data synchronization. High availability is provided by storing multiple copies of databases. Business continuity and disaster recovery is provided by backups and geo-replication, elastic scale, and rapid provisioning. Also, it has built-in data protection and security features.

Prerequisites

- Microsoft Azure Subscription (MSDN subscribers or sign up for one month free trial)

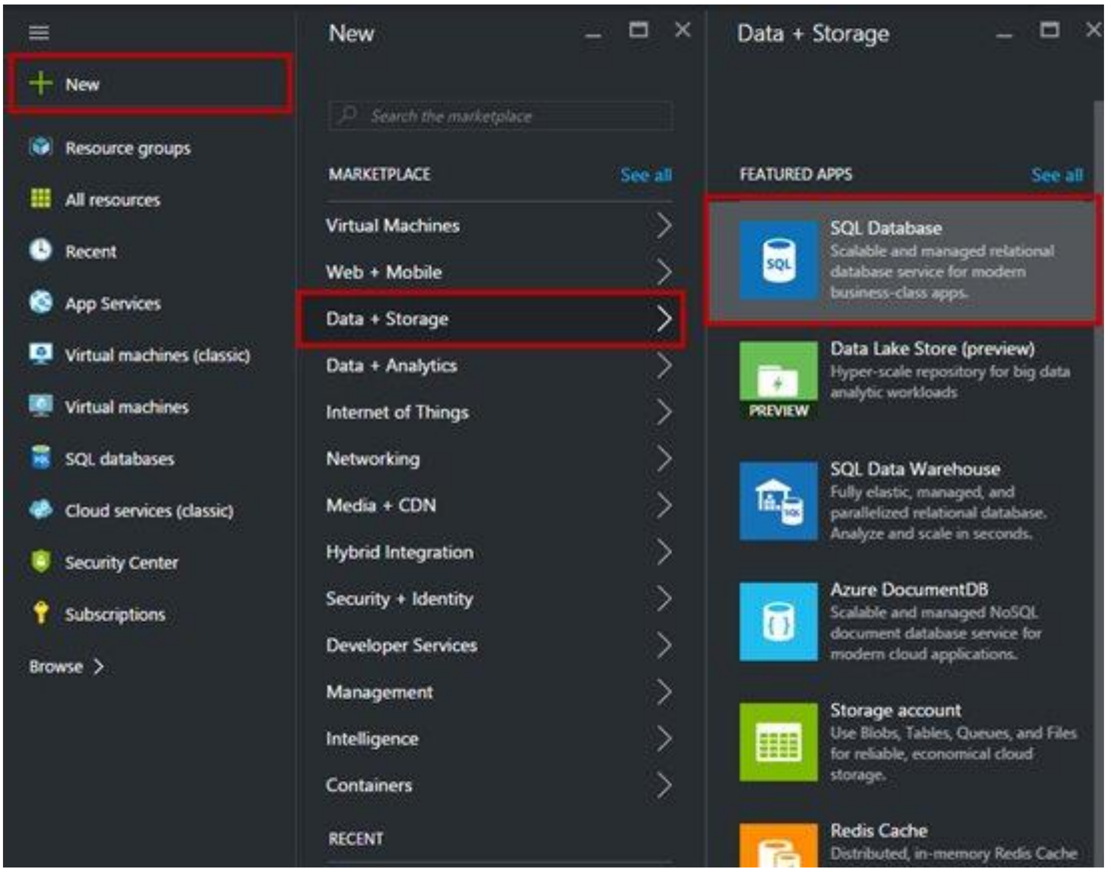
You will learn the following:

- How to create SQL Server
- How to create SQL Database

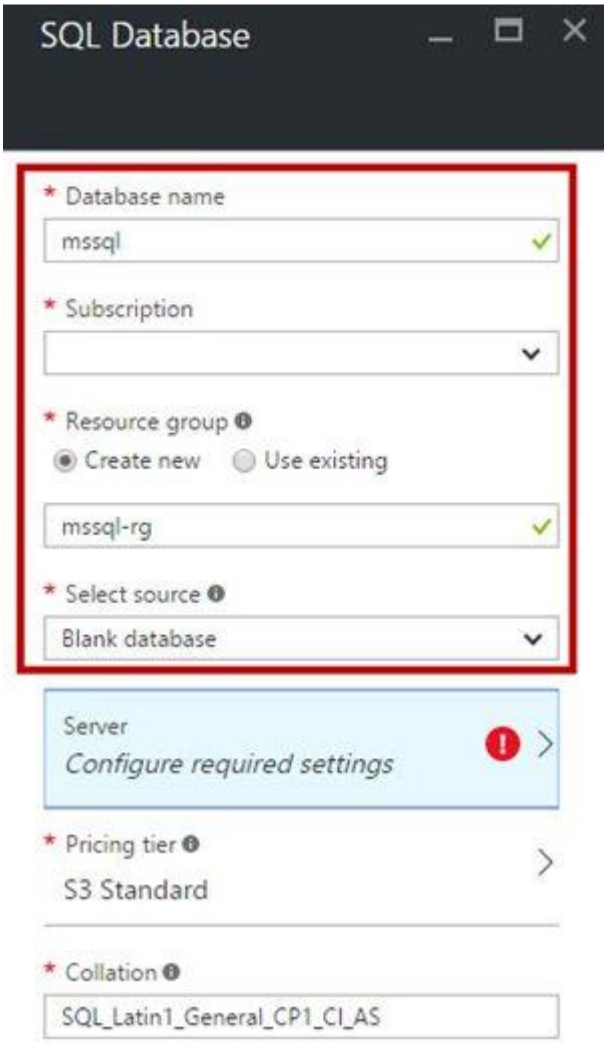
Getting started with SQL Database

Step 1: Navigate to Azure Portal & Sign in with Microsoft Azure credentials.

Step 2: Click on +New -> Data + Storage -> SQL Database.



Step 3: Enter the SQL **Database Name**, choose **Subscription**, and select **Resource Group**: Create New or Use Existing.



SQL Database

* Database name
mssql ✓

* Subscription

* Resource group
● Create new ○ Use existing
mssql-rg ✓

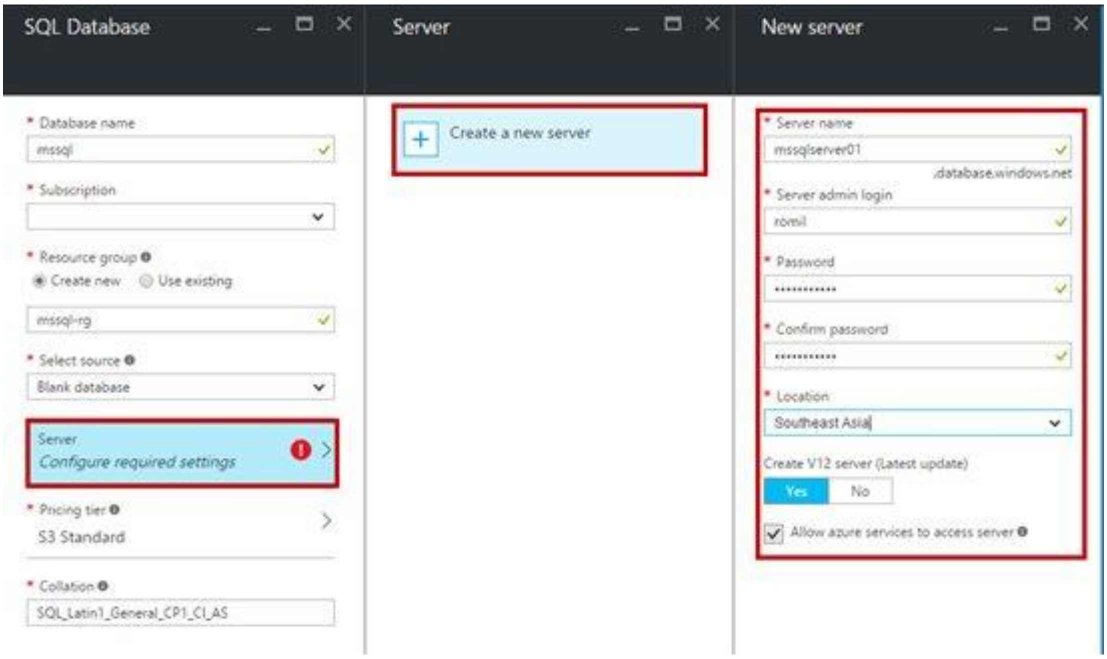
* Select source
Blank database

Server
Configure required settings

* Pricing tier
S3 Standard

* Collation
SQL_Latin1_General_CP1_CI_AS

Step 4: Now, it is time to create Server for database. Click on **Create a new server** option. Again, enter Server Name, Server Admin, Password, and Location.



SQL Database

* Database name
mssql ✓

* Subscription

* Resource group
● Create new ○ Use existing
mssql-rg ✓

* Select source
Blank database

Server
Configure required settings

* Pricing tier
S3 Standard

* Collation
SQL_Latin1_General_CP1_CI_AS

Server

Create a new server

New server

* Server name
mssqlserver01 ✓
.database.windows.net

* Server admin login
romil ✓

* Password
•••••••••••• ✓

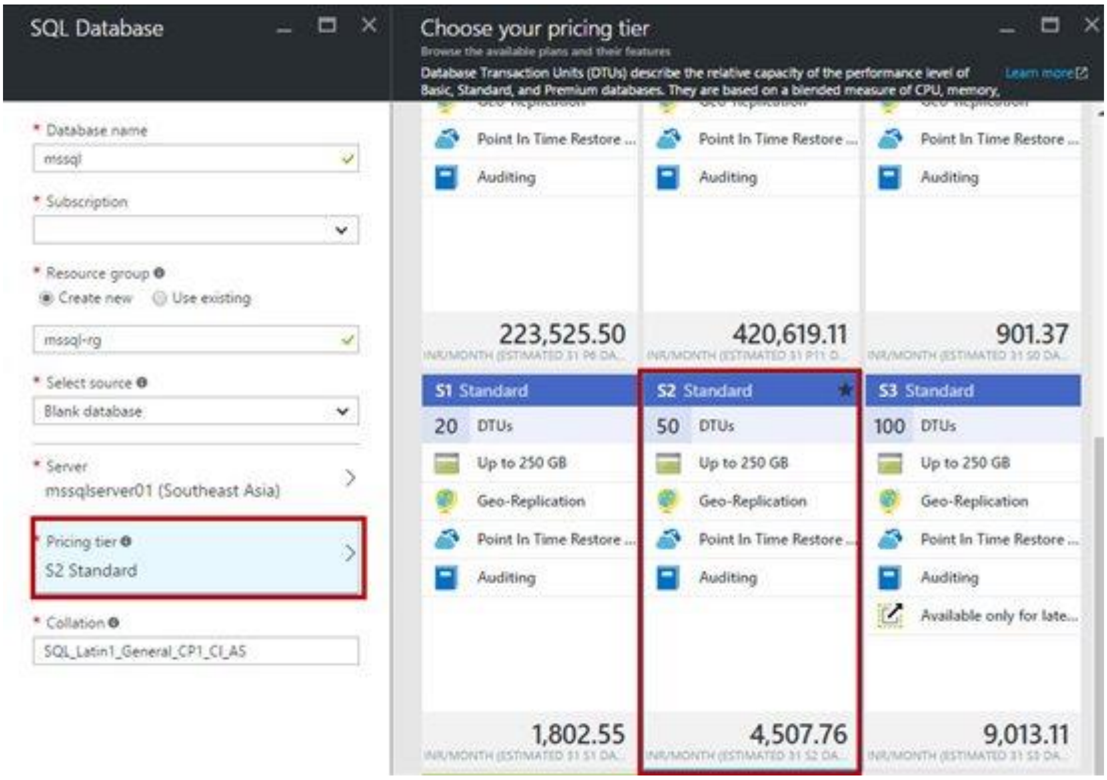
* Confirm password
•••••••••••• ✓

* Location
Southeast Asia

Create V12 server (Latest update)
Yes No

☑ Allow azure services to access server

Step 5: Choose Pricing Tier from Basic, Standard or Premium.



SQL Database

* Database name
mssql

* Subscription

* Resource group
● Create new ○ Use existing
mssql-rg

* Select source
Blank database

* Server
mssqlserver01 (Southeast Asia)

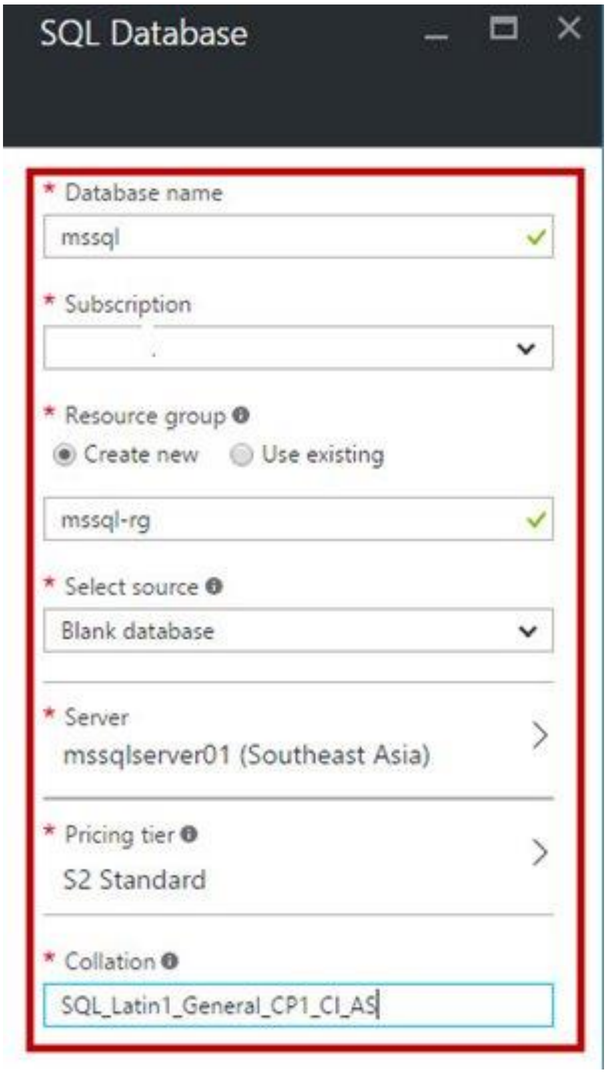
* Pricing tier
S2 Standard

* Collation
SQL_Latin1_General_CP1_CI_AS

Choose your pricing tier
Browse the available plans and their features
Database Transaction Units (DTUs) describe the relative capacity of the performance level of Basic, Standard, and Premium databases. They are based on a blended measure of CPU, memory,
Learn more

Point In Time Restore ...	Point In Time Restore ...	Point In Time Restore ...
Auditing	Auditing	Auditing
223,525.50 INR/MONTH (ESTIMATED 31 P6 DA...	420,619.11 INR/MONTH (ESTIMATED 31 P11 D...	901.37 INR/MONTH (ESTIMATED 31 S0 DA...
S1 Standard	S2 Standard ★	S3 Standard
20 DTUs	50 DTUs	100 DTUs
Up to 250 GB	Up to 250 GB	Up to 250 GB
Geo-Replication	Geo-Replication	Geo-Replication
Point In Time Restore ...	Point In Time Restore ...	Point In Time Restore ...
Auditing	Auditing	Auditing
		Available only for late...
1,802.55 INR/MONTH (ESTIMATED 31 S1 DA...	4,507.76 INR/MONTH (ESTIMATED 31 S2 DA...	9,013.11 INR/MONTH (ESTIMATED 31 S3 DA...

Step 6: Summary of the SQL Database options is available below:



* Database name

mssql

* Subscription

* Resource group

● Create new ○ Use existing

mssql-rg

* Select source

Blank database

* Server

mssqlserver01 (Southeast Asia)

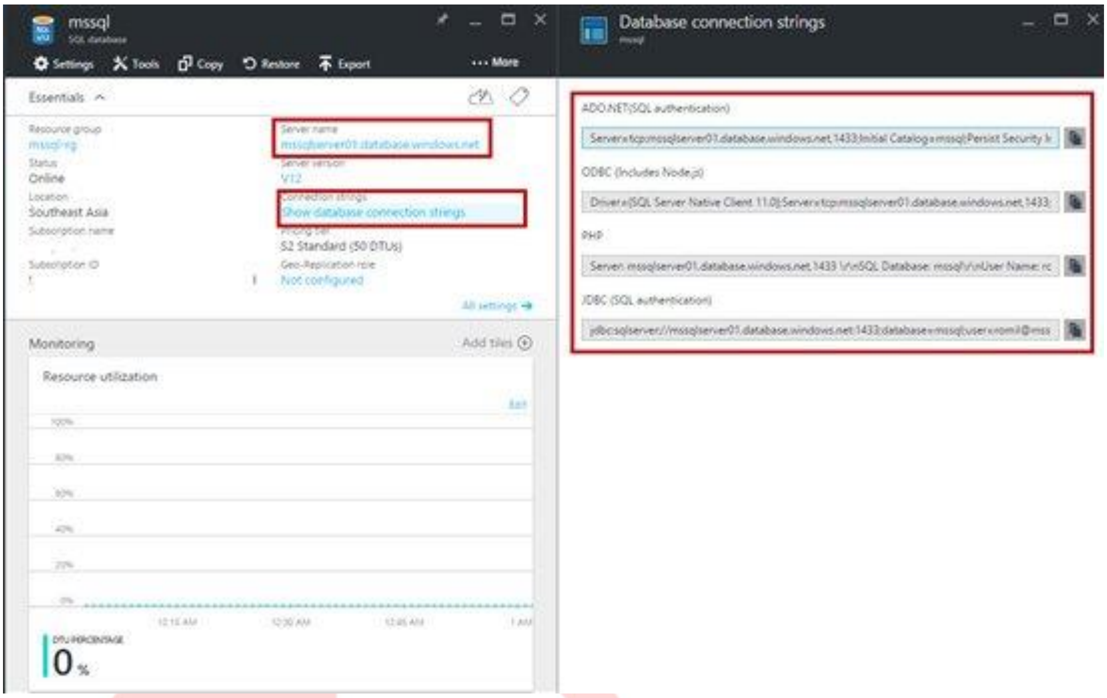
* Pricing tier

S2 Standard

* Collation

SQL_Latin1_General_CP1_CI_AS

Step 7: Wait for a few seconds to let the SQL Database on Azure get created. To use SQL Database in the application, we need to use connection string. All connection strings for other databases, such as ADO.NET, ODBC, PHP, JDBC, can be seen here,



Resource group
mssql-rg
Status
Online
Location
Southeast Asia
Subscription name

Subscription ID

Server name
mssqlserver01.database.windows.net
Server version
V12
Connection strings
Show database connection strings
Pricing tier
S2 Standard (50 DTUs)
Geo-Replication role
Not configured

All settings →

ADO.NET(SQL authentication)

```
Server=tcp:mssqlserver01.database.windows.net,1433;Initial Catalog=mssql;Persist Security In
```

ODBC (Includes Node.js)

```
Driver={SQL Server Native Client 11.0};Server=tcp:mssqlserver01.database.windows.net,1433;
```

PHP

```
Server: mssqlserver01.database.windows.net,1433 \r\nSQL Database: mssql\r\nUser Name: rc
```

JDBC (SQL authentication)

```
jdbc:sqlserver://mssqlserver01.database.windows.net:1433;database=mssql;user=romil@mss
```

SQL Database – Set firewall client IP for SQL Server

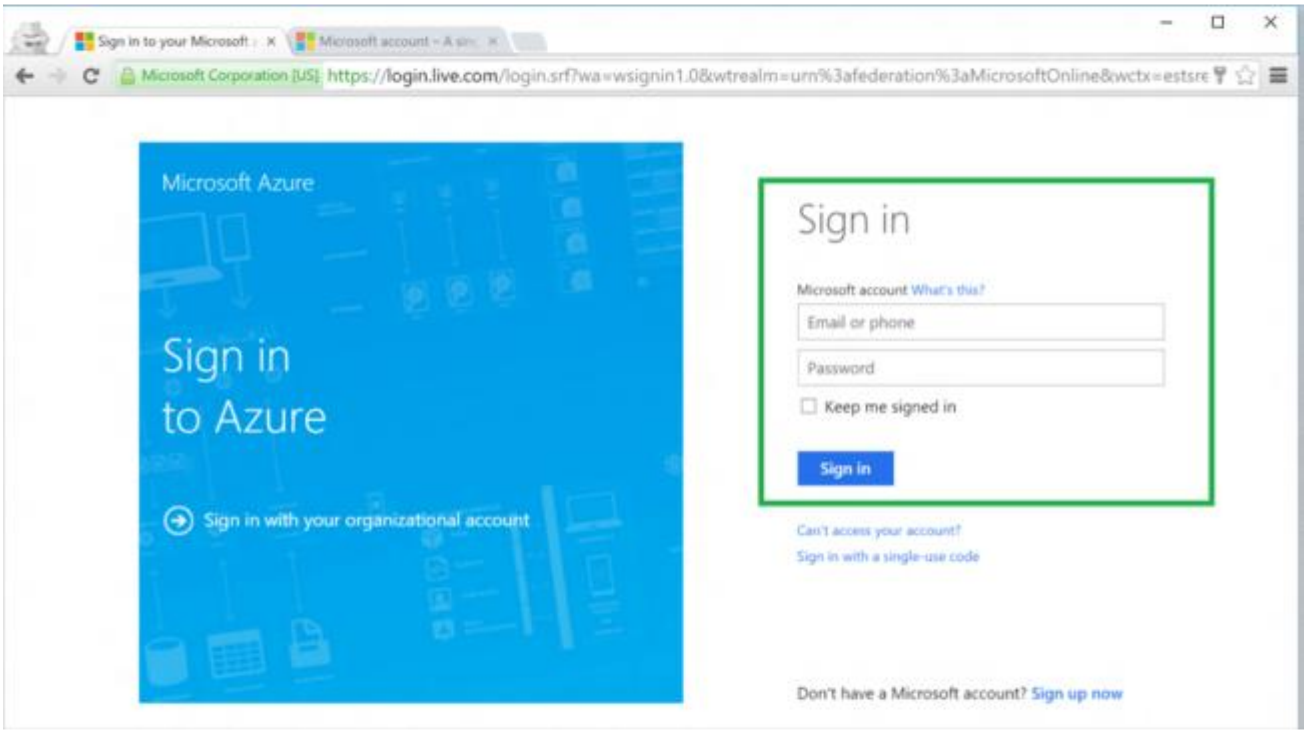
Prerequisites

- Azure account.

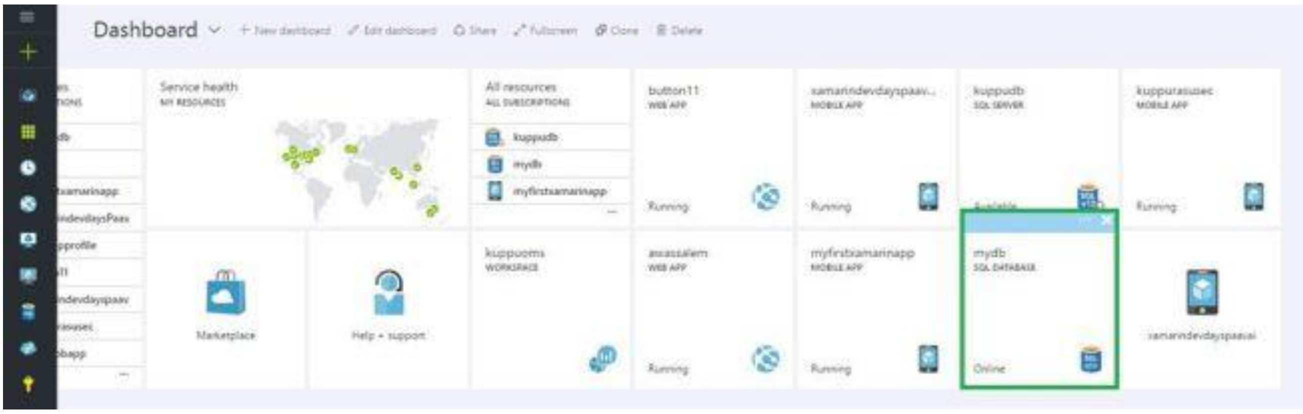
Now, let's get started with the steps, given below-

Create a new Azure SQL Server-level Firewall.

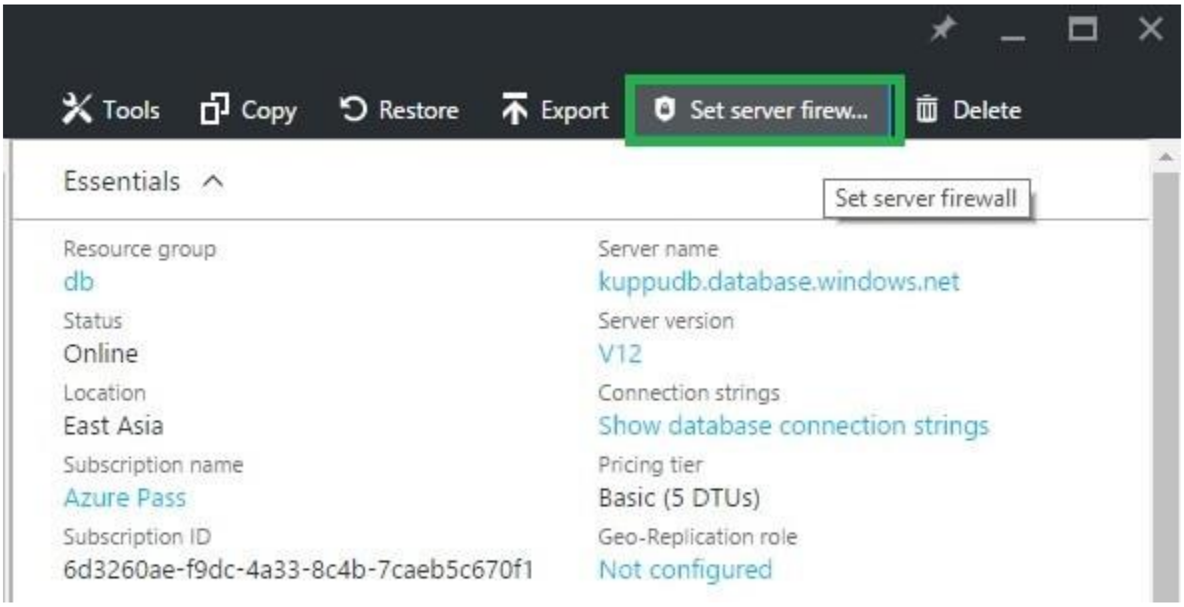
Step 1- Sign in to the online Microsoft Azure Portal.


Sign in to your Microsoft
Microsoft account - A sin
Microsoft Corporation [US]
https://login.live.com/login.srf?wa=wsignin1.0&wtrealm=urn%3afederation%3aMicrosoftOnline&wctx=estsre
Microsoft Azure
Sign in
to Azure
Sign in with your organizational account
Sign in
Microsoft account What's this?
Email or phone
Password
□ Keep me signed in
Sign in
Can't access your account?
Sign in with a single-use code
Don't have a Microsoft account? Sign up now

Step 2- In the dashboard, click SQL Servers.



Step 3- Next, on SQL Servers blade, click the Server on which Firewall rule is to be created.



Essentials

Resource group
db

Status
Online

Location
East Asia

Subscription name
Azure Pass

Subscription ID
6d3260ae-f9dc-4a33-8c4b-7caeb5c670f1

Server name
kuppudb.database.windows.net

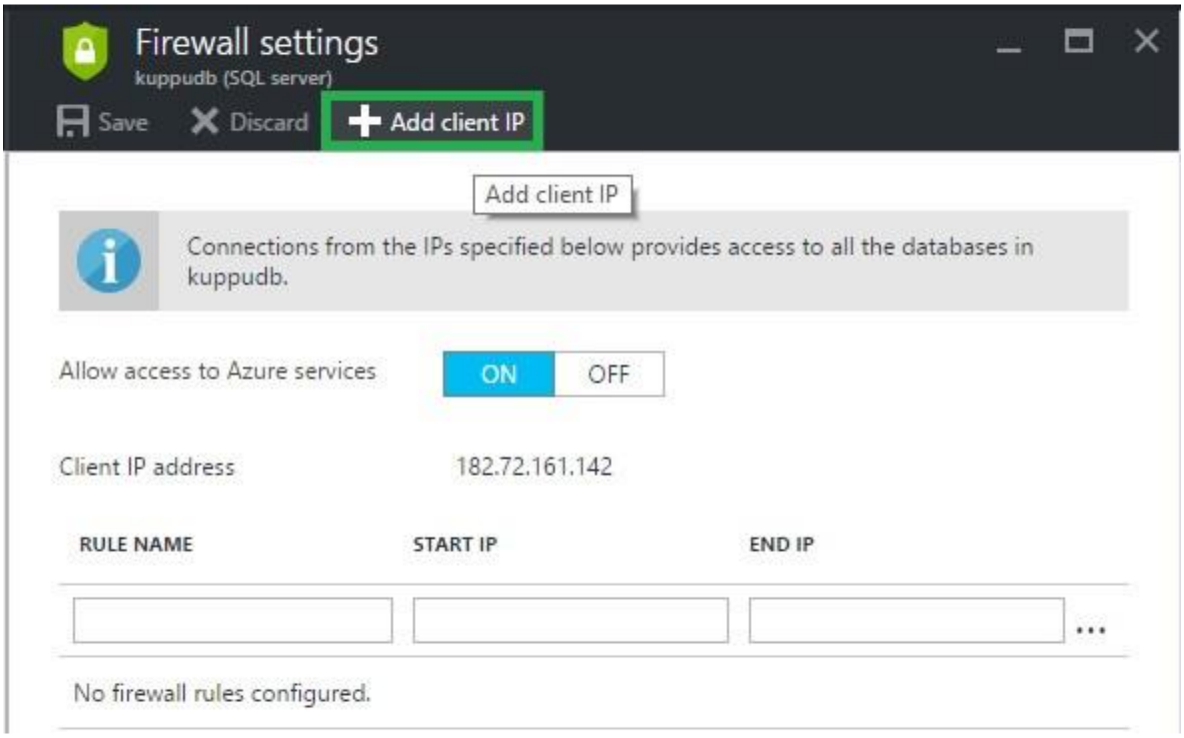
Server version
V12

Connection strings
Show database connection strings

Pricing tier
Basic (5 DTUs)

Geo-Replication role
Not configured

Step 4- Now, click Add client IP to have Azure create a rule for your client IP address.



Firewall settings
kuppudb (SQL server)

Connections from the IPs specified below provides access to all the databases in kuppudb.

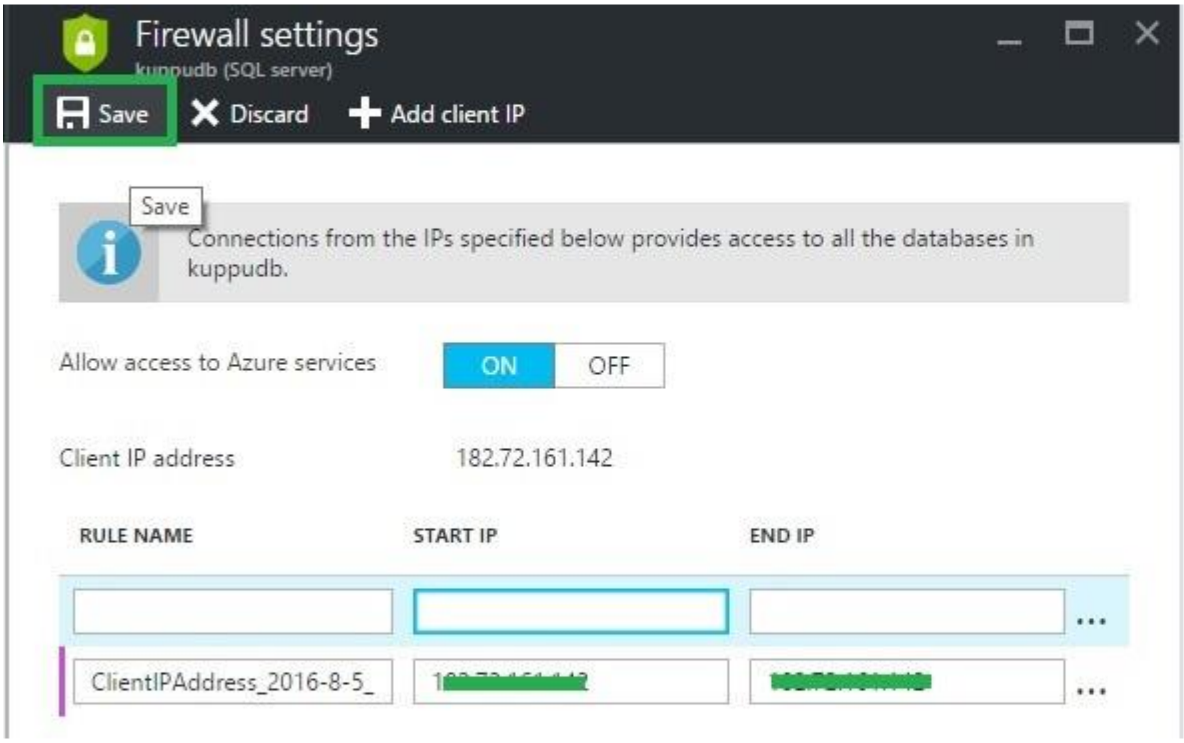
Allow access to Azure services: ON

Client IP address: 182.72.161.142

RULE NAME	START IP	END IP

No firewall rules configured.

Step 5- Finally, click Save to create the Server-level Firewall rule.



Firewall settings

kuppudb (SQL server)

Connections from the IPs specified below provides access to all the databases in kuppudb.

Allow access to Azure services [✓ ON] OFF

Client IP address 182.72.161.142

RULE NAME	START IP	END IP
ClientIPAddress_2016-8-5_	[redacted]	[redacted]

Optionally, to allow access to a range of IP addresses, click the IP address, which was added to edit Firewall address.

Summary

In this article, we discussed, how to create new Azure SQL Server-level Firewall, using Azure Portal.

Dynamic Data Masking:

Overview

An Azure SQL Database Dynamic Data Masking limits the sensitive data exposure by masking it to non-privileged users. The dynamic data masking is supported for the V12 version of Azure SQL Database.

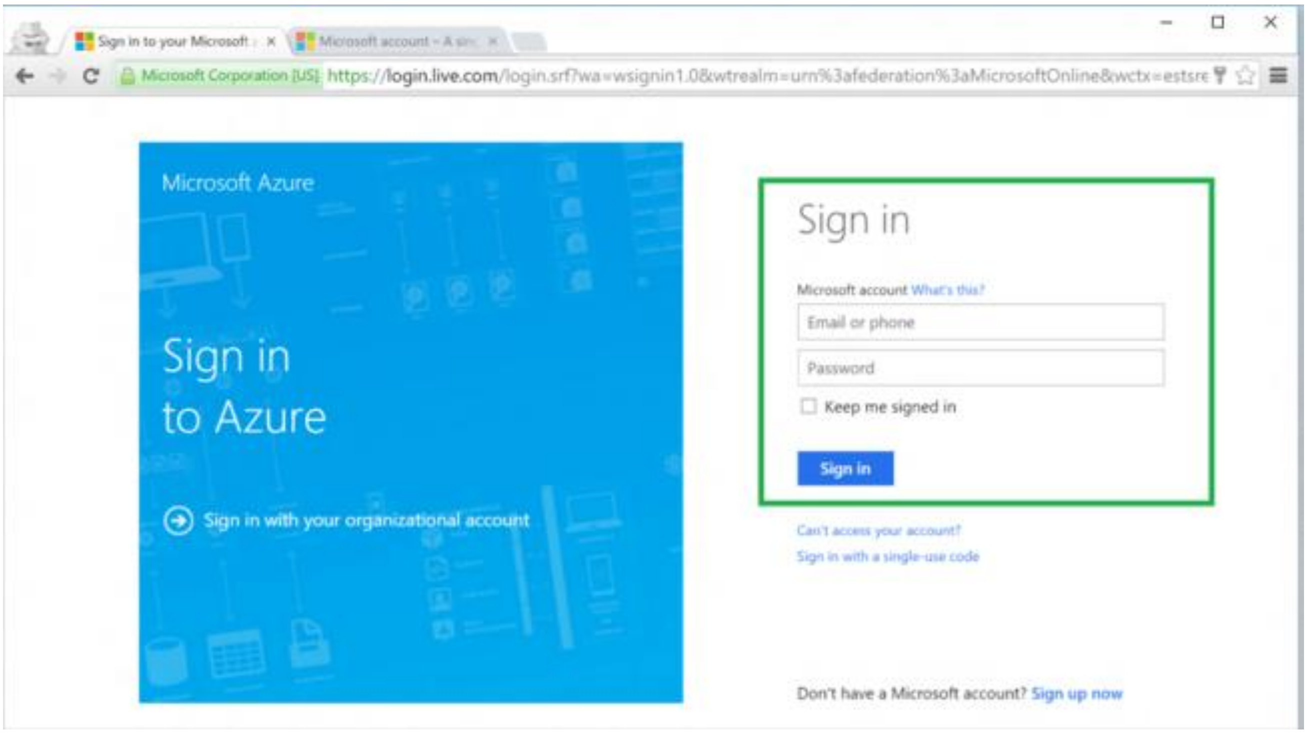
Prerequisites

- Azure account.

Now, let's get started with the following steps -

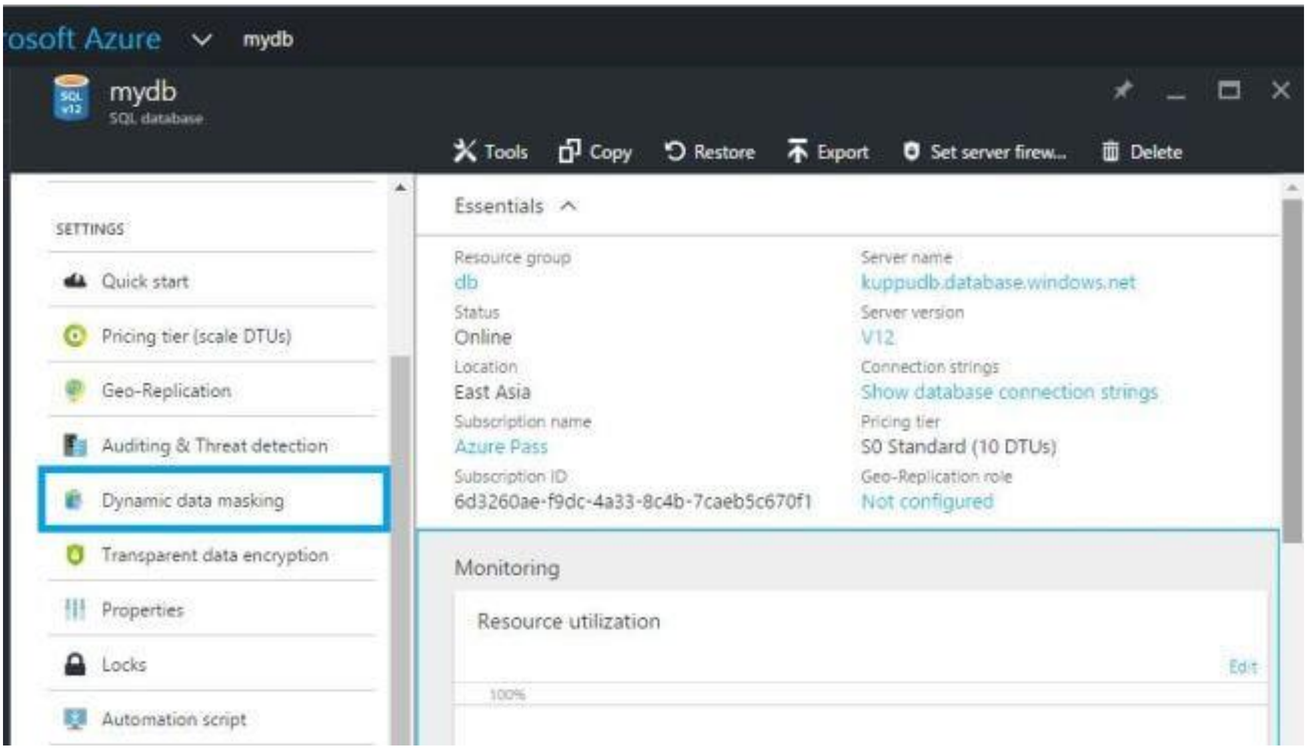
Set up dynamic data masking for your database, using the Azure Portal

Sign in to the online Microsoft Azure Portal.


Sign in to your Microsoft
Microsoft account - A sin
Microsoft Corporation [US]
Microsoft Azure
Sign in
to Azure
Sign in with your organizational account
Sign in
Microsoft account What's this?
Email or phone
Password
□ Keep me signed in
Sign in
Can't access your account?
Sign in with a single-use code
Don't have a Microsoft account? Sign up now

https://login.live.com/login.srf?wa=wsignin1.0&wtrealm=urn%3afederation%3aMicrosoftOnline&wctx=estsre

Open the existing database on Azure portal. Click the Dynamic Data Masking tile which launches the Dynamic Data Masking configuration blade.



Resource group
db

Status
Online

Location
East Asia

Subscription name
Azure Pass

Subscription ID
6d3260ae-f9dc-4a33-8c4b-7caeb5c670f1

Server name
kuppudb.database.windows.net

Server version
V12

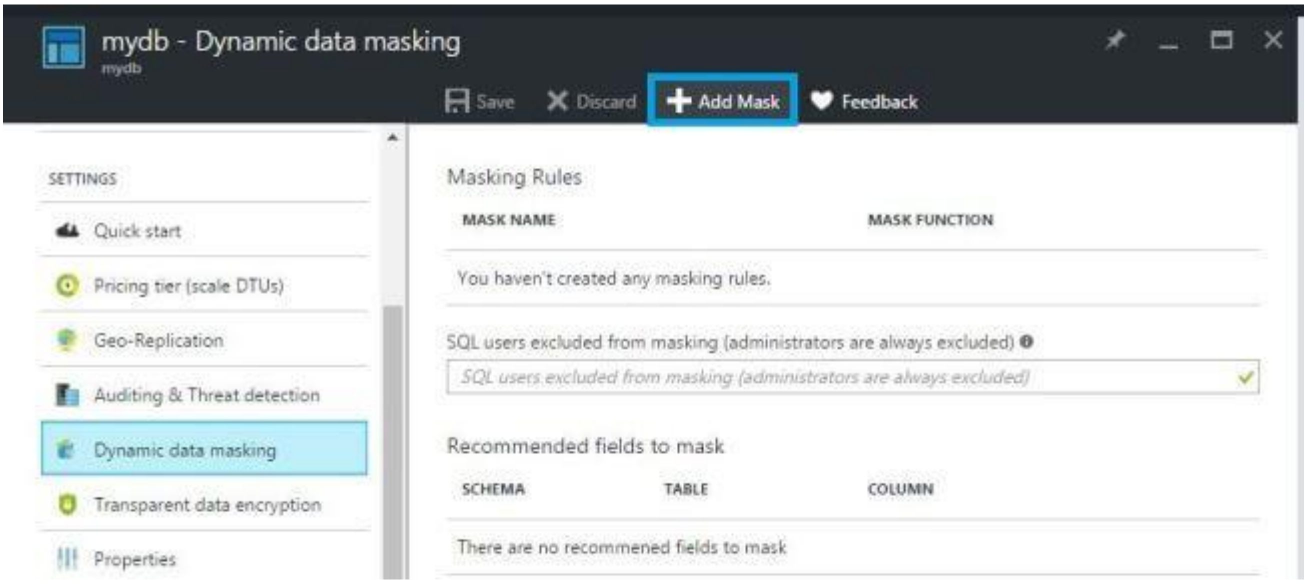
Connection strings
Show database connection strings

Pricing tier
S0 Standard (10 DTUs)

Geo-Replication role
Not configured

In the Dynamic Data Masking configuration blade, we may see some database columns that the recommendations engine has flagged, for masking.

In order to accept the recommendations, just click **Add Mask** for one or more columns and a mask will be created based on the default type for this column.


mydb - Dynamic data masking
mydb
Save
Discard
Add Mask
Feedback
SETTINGS
Quick start
Pricing tier (scale DTUs)
Geo-Replication
Auditing & Threat detection
Dynamic data masking
Transparent data encryption
Properties

Masking Rules

MASK NAME	MASK FUNCTION
You haven't created any masking rules.	

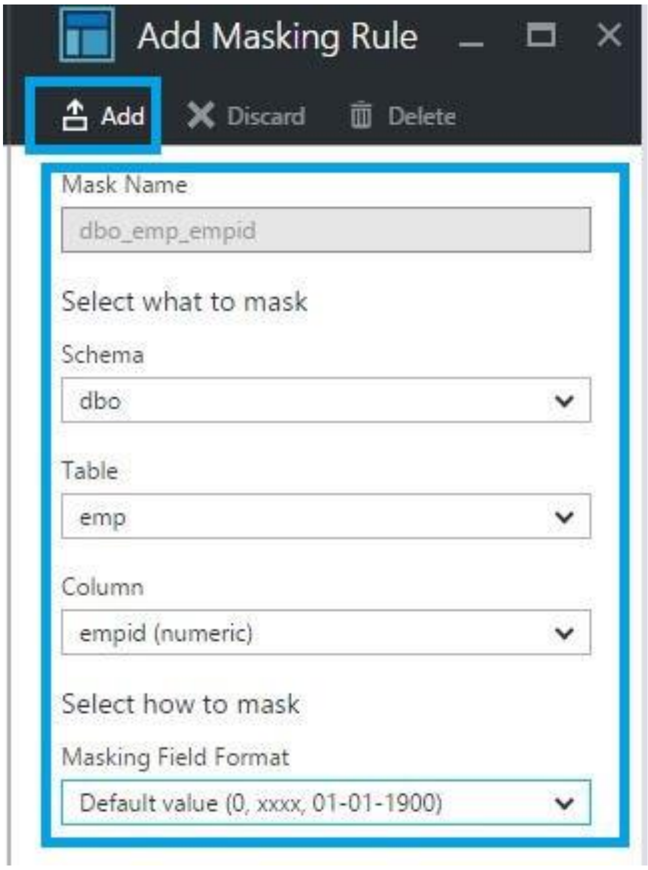
SQL users excluded from masking (administrators are always excluded): *SQL users excluded from masking (administrators are always excluded)*

Recommended fields to mask

SCHEMA	TABLE	COLUMN
There are no recommened fields to mask		

To add a mask for any column in your database, select the Schema, Table, and Column to define the designated field that will be masked.

Choose a Masking Field Format from the list of sensitive data masking categories. Click **Save** in the data masking rule blade, to update the set of masking rules in the dynamic data masking policy.



Mask Name: dbo_emp_empid

Select what to mask

Schema: dbo

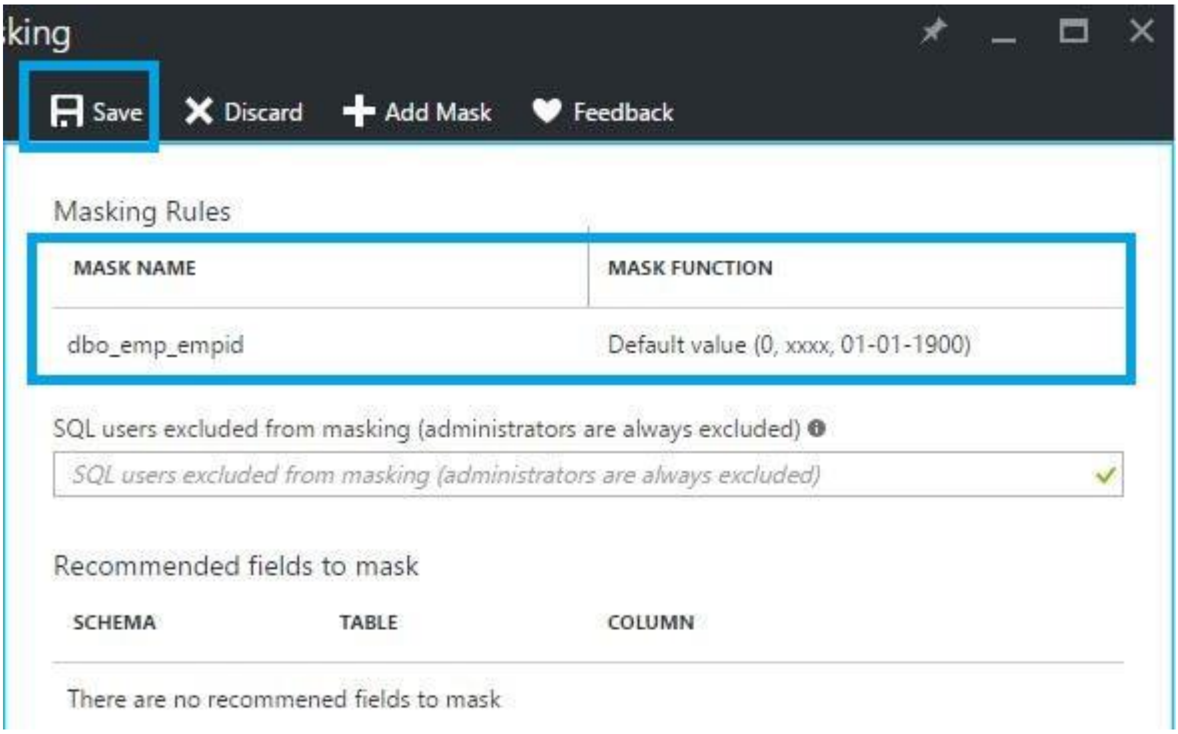
Table: emp

Column: empid (numeric)

Select how to mask

Masking Field Format: Default value (0, xxxx, 01-01-1900)

A few seconds later, the mask function is applied to that particular column.



Masking Rules

MASK NAME	MASK FUNCTION
dbo_emp_empid	Default value (0, xxxx, 01-01-1900)

SQL users excluded from masking (administrators are always excluded)

SQL users excluded from masking (administrators are always excluded)

Recommended fields to mask

SCHEMA	TABLE	COLUMN
There are no recommened fields to mask		

Scaling with your SQL Database:

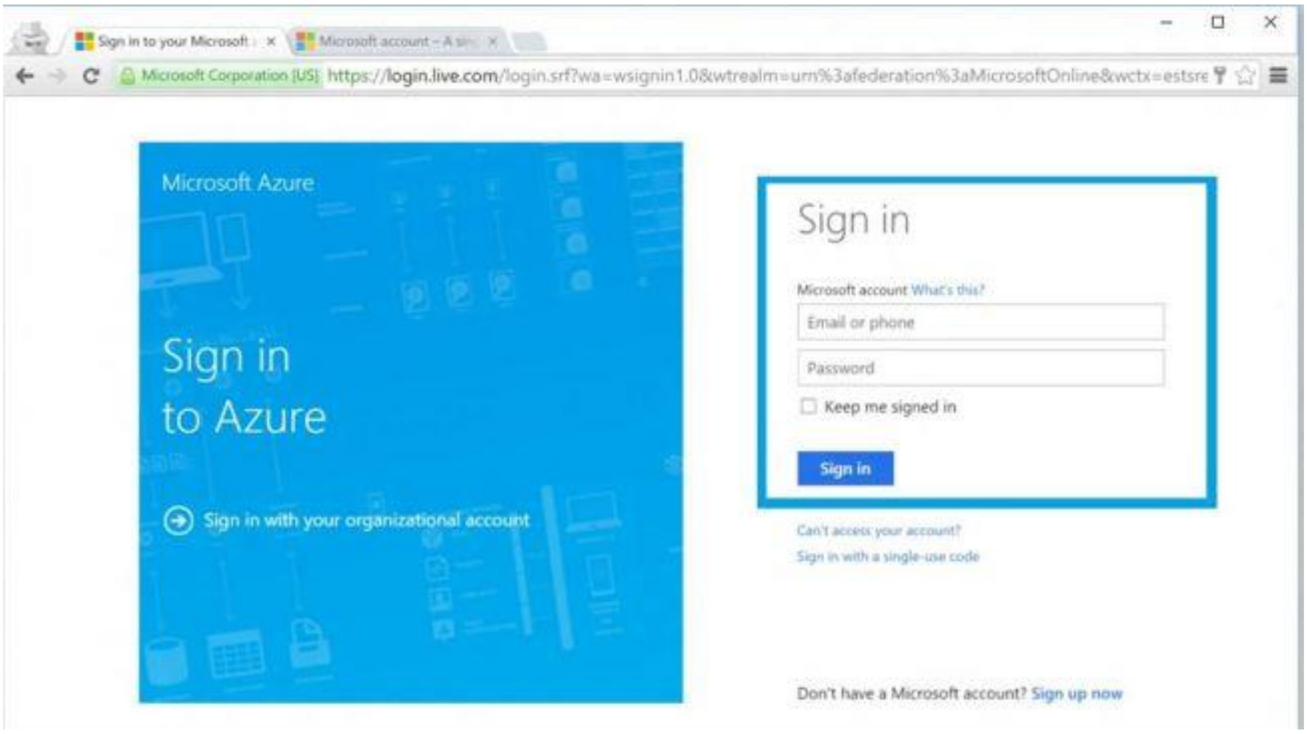
SQL Database - Scale up your SQL DB size on Azure

Prerequisites

- Azure account.

Now, let's get started with the steps, given below-

Step 1- Sign in to the online Microsoft Azure Portal.



Sign in to your Microsoft | Microsoft account - A si

Microsoft Corporation [US] https://login.live.com/login.srf?wa=wsignin1.0&wtrealm=urn%3afederation%3aMicrosoftOnline&wctx=estsre

Microsoft Azure

Sign in to Azure

Sign in with your organizational account

Sign in

Microsoft account What's this?

Email or phone

Password

□ Keep me signed in

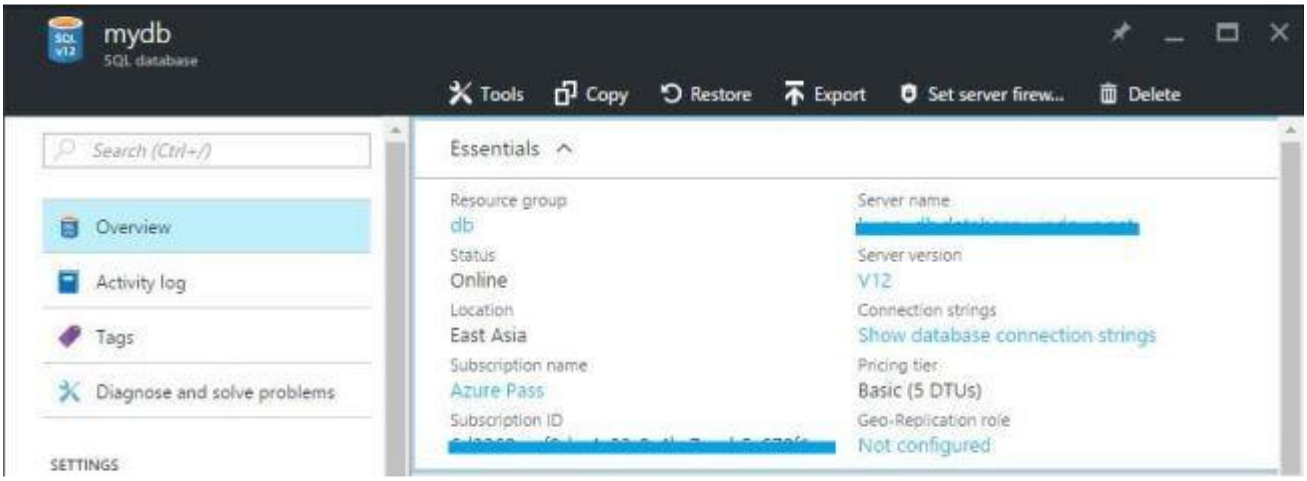
Sign in

Can't access your account?

Sign in with a single-use code

Don't have a Microsoft account? Sign up now

On the SQL Servers blade, navigate to the monitoring blade of SQL database.



mydb
SQL database

Tools | Copy | Restore | Export | Set server firew... | Delete

Search (Ctrl+/)

- Overview
- Activity log
- Tags
- Diagnose and solve problems

SETTINGS

Essentials

Resource group: db

Status: Online

Location: East Asia

Subscription name: Azure Pass

Subscription ID: [redacted]

Server name: [redacted]

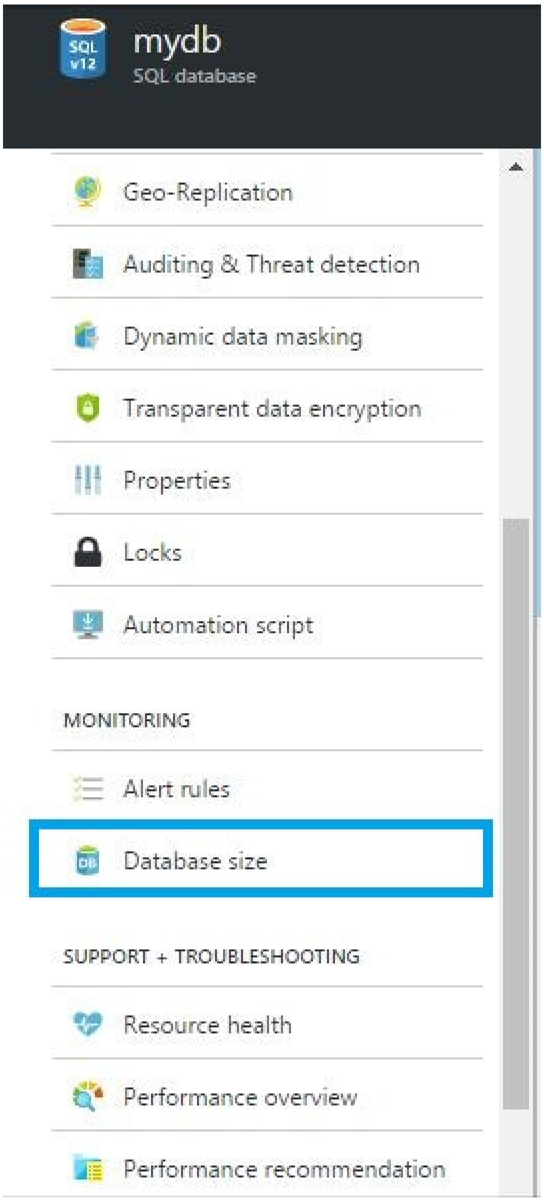
Server version: V12

Connection strings: Show database connection strings

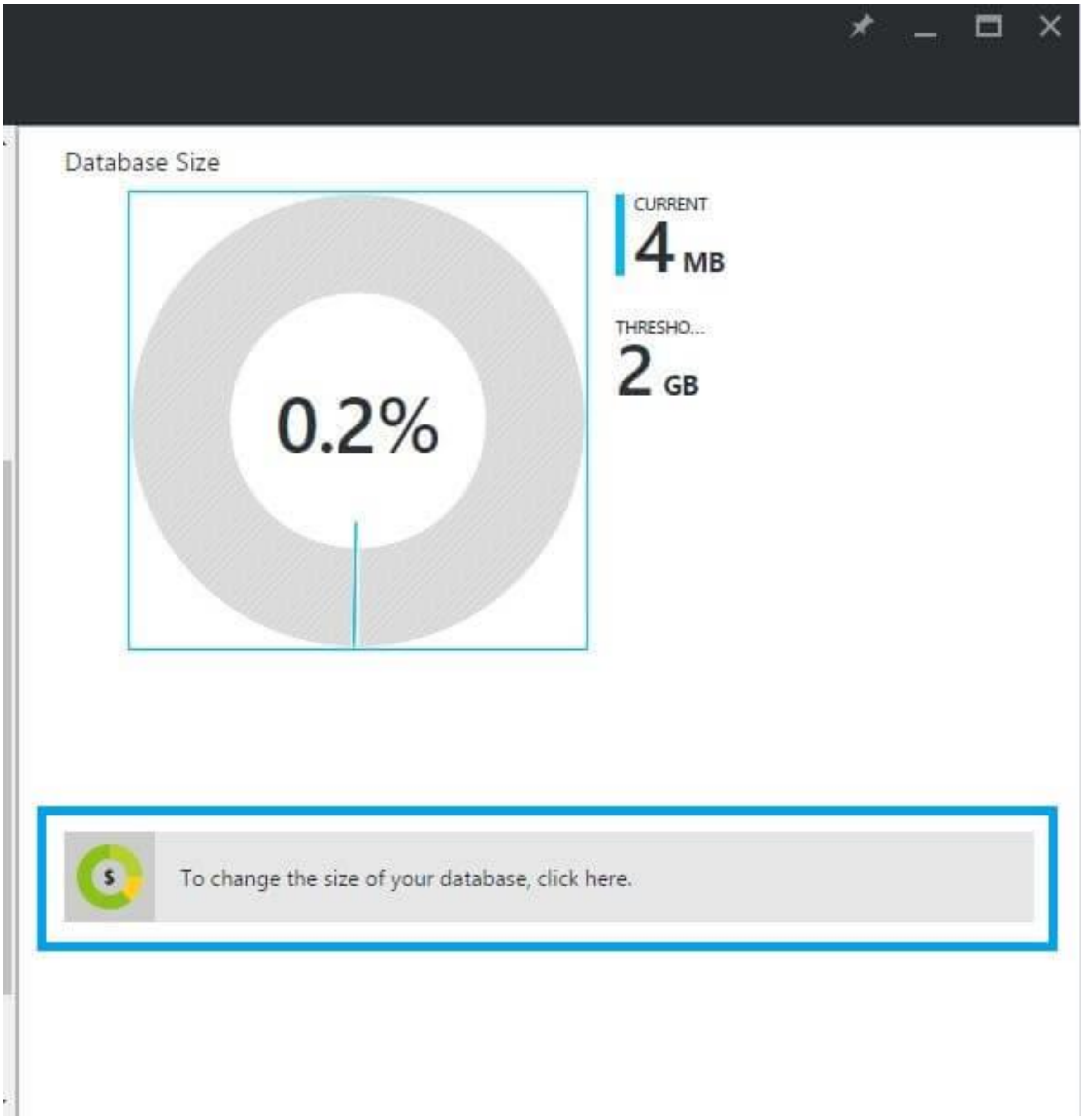
Pricing tier: Basic (5 DTUs)

Geo-Replication role: Not configured

Click Database Size option, which will display the monitoring settings.



Click Here button needs to be clicked.



Database Size

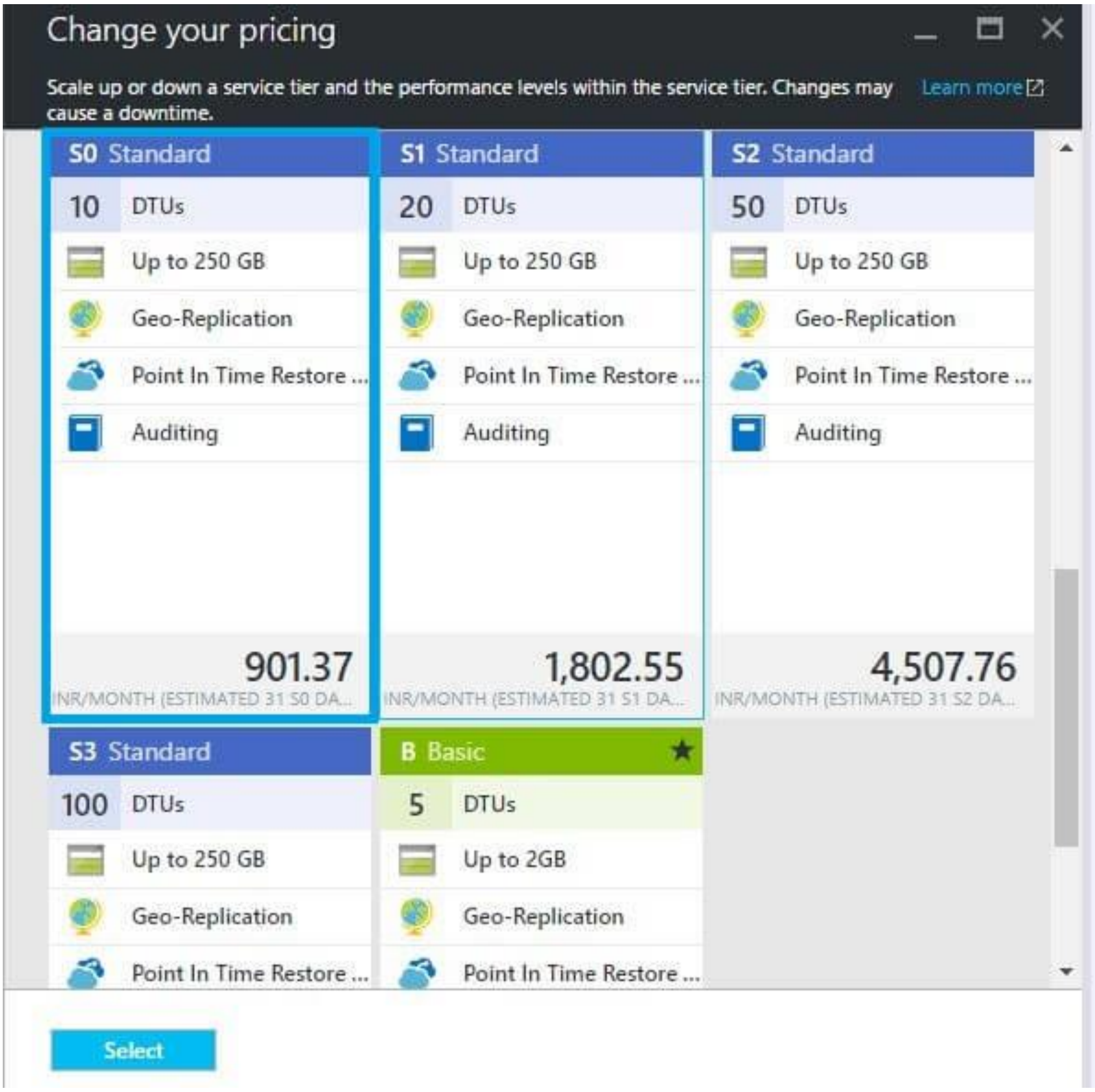
0.2%

CURRENT 4 MB

THRESHO... 2 GB

To change the size of your database, click here.

Finally, we change the database size in the Service tier.



Change your pricing

Scale up or down a service tier and the performance levels within the service tier. Changes may cause a downtime.

S0 Standard	S1 Standard	S2 Standard	S3 Standard	B Basic ★
10 DTUs	20 DTUs	50 DTUs	100 DTUs	5 DTUs
Up to 250 GB	Up to 250 GB	Up to 250 GB	Up to 250 GB	Up to 2GB
Geo-Replication	Geo-Replication	Geo-Replication	Geo-Replication	Geo-Replication
Point In Time Restore ...	Point In Time Restore ...	Point In Time Restore ...	Point In Time Restore ...	Point In Time Restore ...
Auditing	Auditing	Auditing		
901.37 INR/MONTH (ESTIMATED 31 S0 DA...	1,802.55 INR/MONTH (ESTIMATED 31 S1 DA...	4,507.76 INR/MONTH (ESTIMATED 31 S2 DA...		

We will receive the notification and our database size will be changed.

SQL Database - Threat Detection

Overview

Threat detection detects abnormal database activities indicating potential security threats to the database and offers a new layer of security, which enables the customers to detect and respond to the potential threats as they occur by providing security alerts on abnormal activities. The customers can explore suspicious events, using Azure SQL database auditing to determine, if they result from an attempt to access, breach or exploit the data in the database. Threat detection makes it simple to address possible threats to the database without the need to be a security expert or manage advanced security monitoring systems.

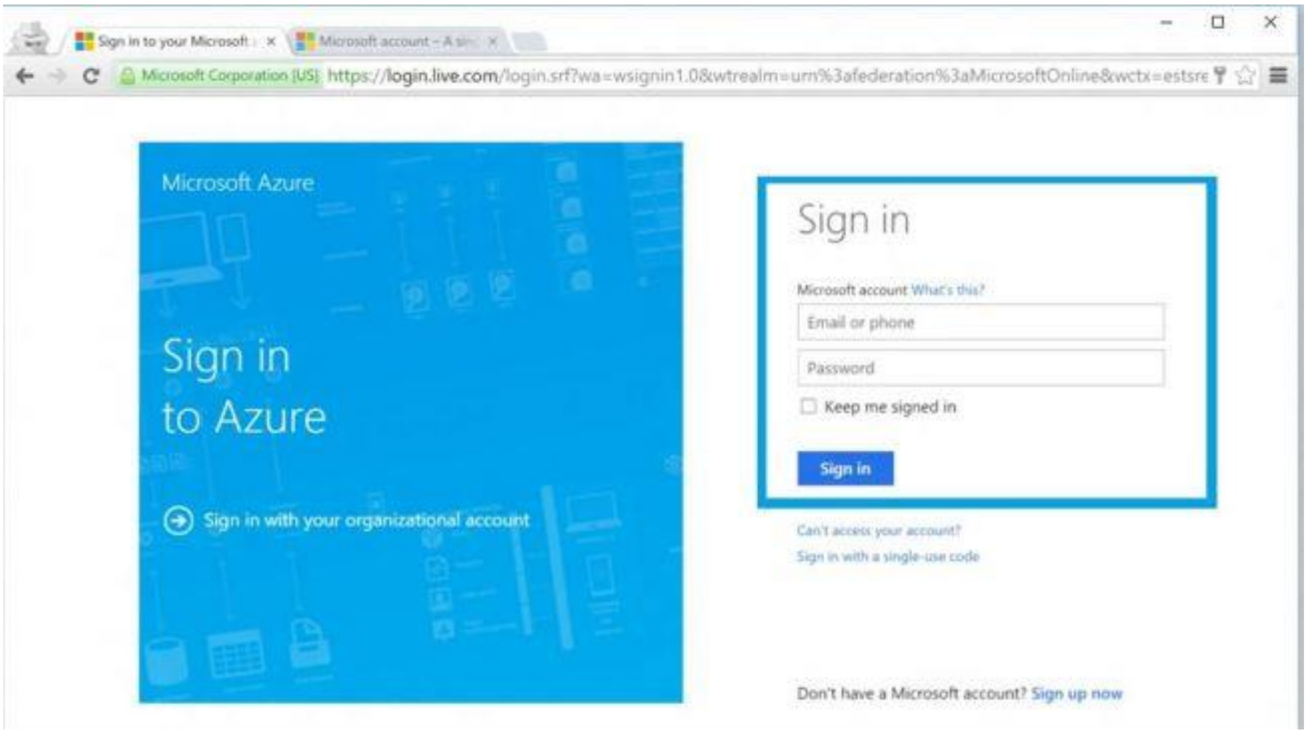
For example, Threat detection detects certain abnormal database activities, thereby specifying the potential SQL injection attempts. SQL injection is one of the common Web Application security problems on the Internet, used to attack data-driven Applications. The attackers take advantage of the Application vulnerabilities to inject malicious SQL statements into Application entry fields, for breaching or modifying the data in the database.

Prerequisites

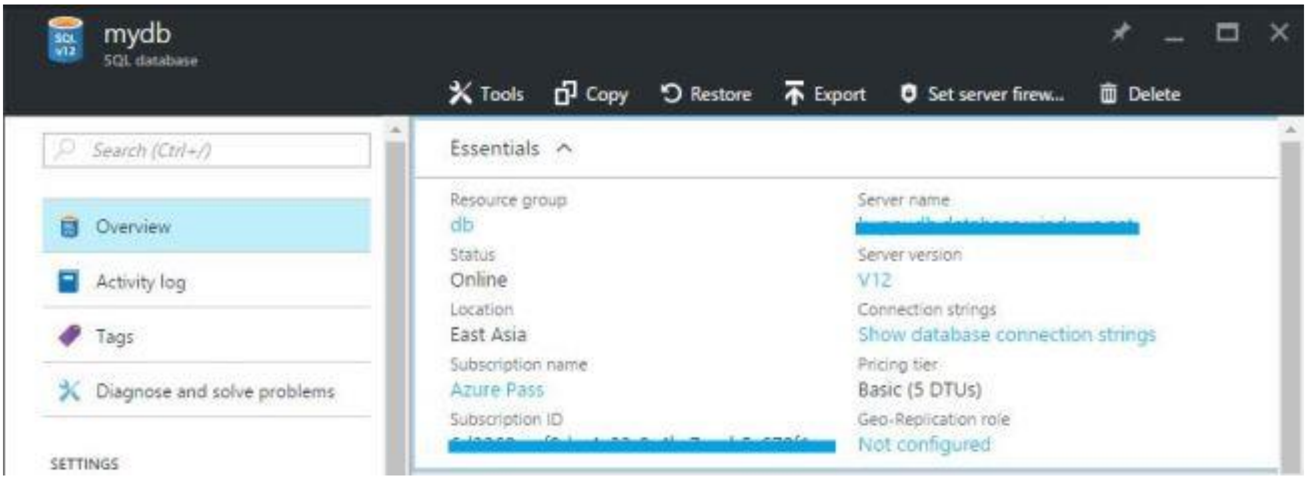
- Azure account.

Now, let's get started with the steps, given below-

Step 1- Sign in to the online Microsoft Azure Portal.


Sign in to your Microsoft
Microsoft account – A sin
Microsoft Corporation [US]
https://login.live.com/login.srf?wa=wsignin1.0&wtrealm=urn%3afederation%3aMicrosoftOnline&wctx=estsre
Microsoft Azure
Sign in
to Azure
Sign in with your organizational account
Sign in
Microsoft account What's this?
Email or phone
Password
□ Keep me signed in
Sign in
Can't access your account?
Sign in with a single-use code
Don't have a Microsoft account? Sign up now

On SQL Servers blade, navigate to the configuration blade of SQL database.



Resource group
db

Status
Online

Location
East Asia

Subscription name
Azure Pass

Subscription ID
[redacted]

Server name
[redacted]

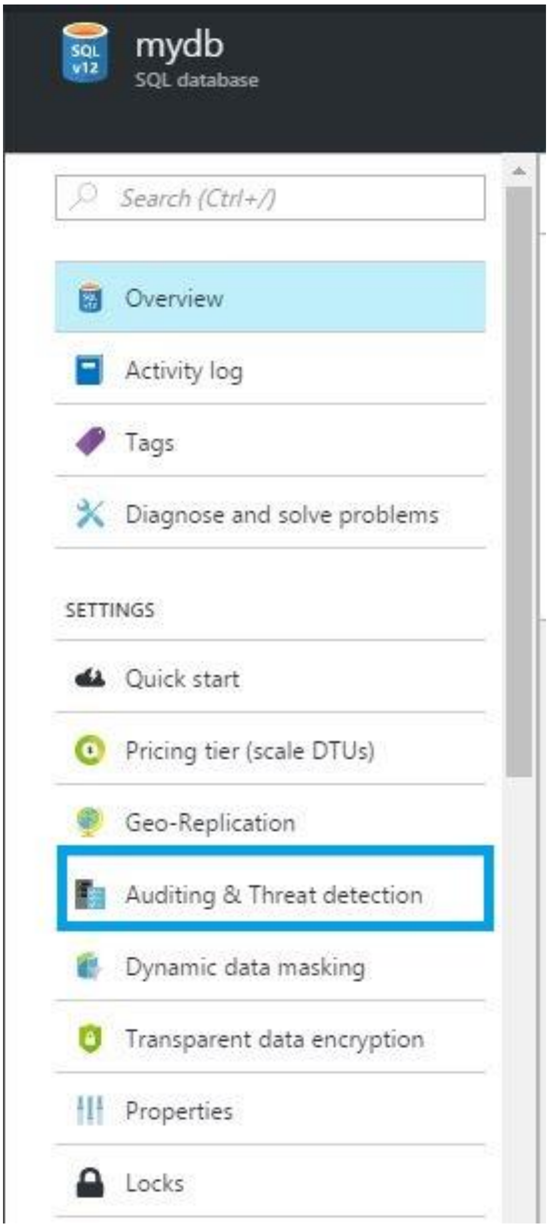
Server version
V12

Connection strings
Show database connection strings

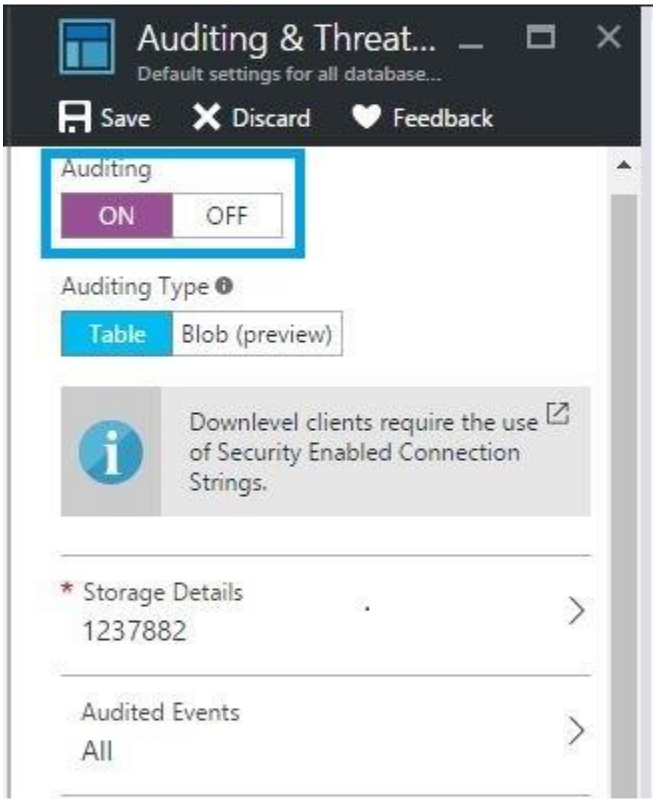
Pricing tier
Basic (5 DTUs)

Geo-Replication role
Not configured

Choose auditing & threat detection option.



In the auditing & threat detection configuration blade, turn ON auditing, which will display the threat detection settings.



Auditing & Threat...

Default settings for all database...

Auditing: ON

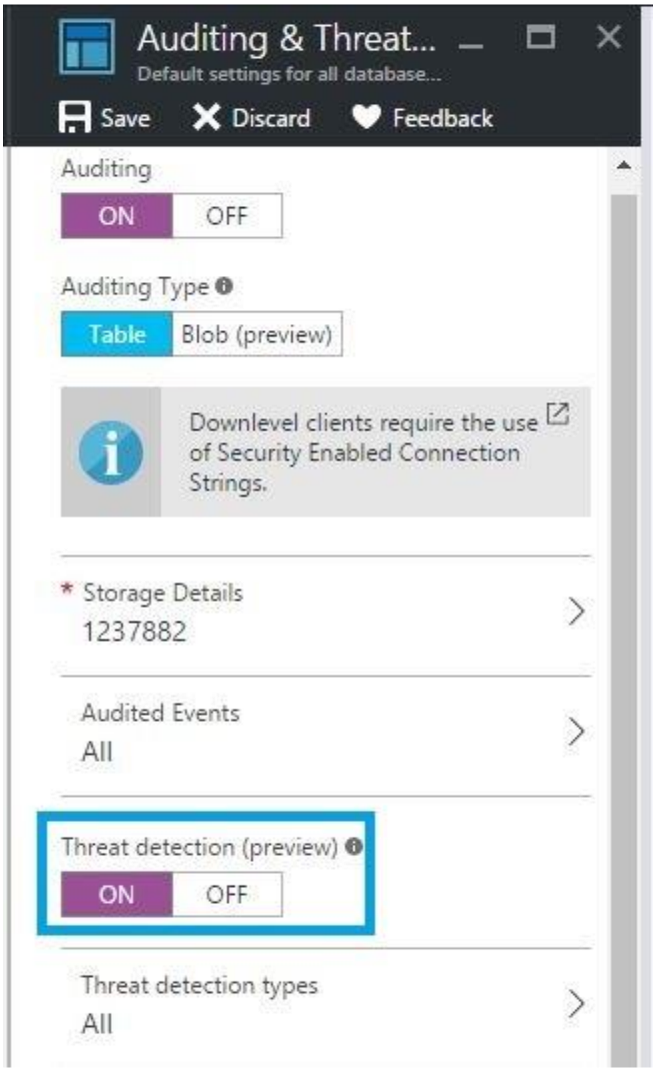
Auditing Type: Table

Downlevel clients require the use of Security Enabled Connection Strings.

* Storage Details: 1237882

Audited Events: All

Turn ON threat detection.



Auditing: ON

Auditing Type: Table

Downlevel clients require the use of Security Enabled Connection Strings.

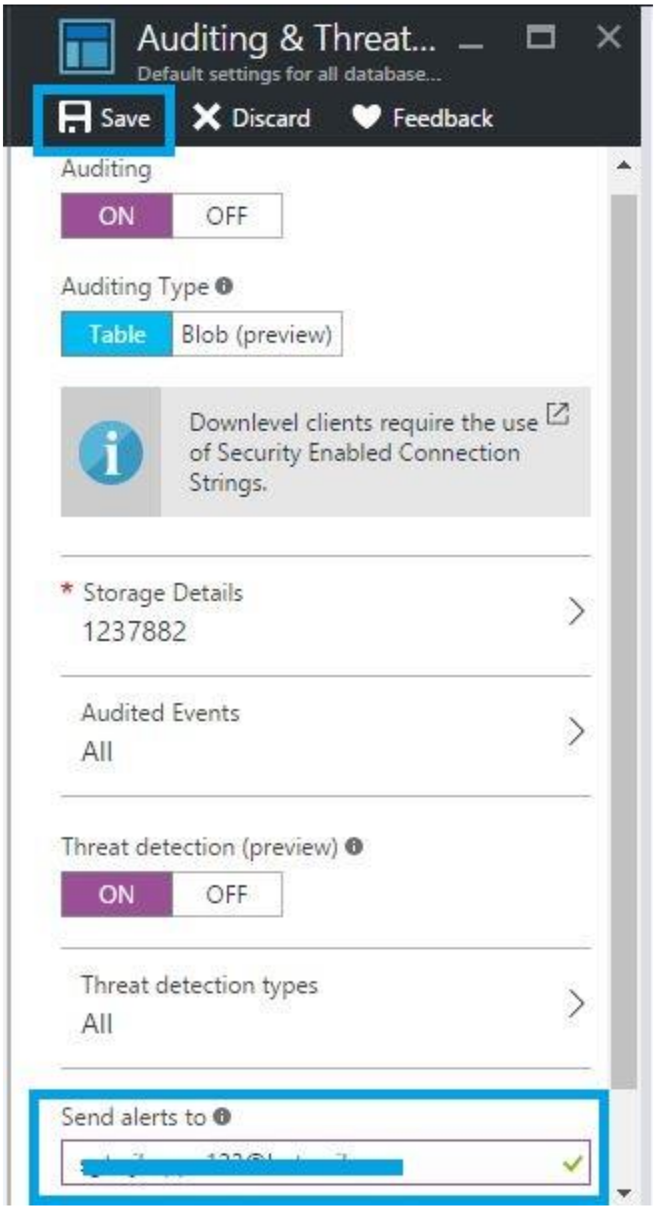
* Storage Details
1237882

Audited Events
All

Threat detection (preview): ON

Threat detection types
All

Finally, type Email ID to get the thread information. Click save in the auditing & threat detection configuration blade to save the new or updated auditing and threat detection policy.



Auditing & Threat...

Default settings for all database...

Auditing

[✓ ON] OFF

Auditing Type

[✓ Table] Blob (preview)

Downlevel clients require the use of Security Enabled Connection Strings.

* Storage Details

1237882

Audited Events

All

Threat detection (preview)

[✓ ON] OFF

Threat detection types

All

Send alerts to

[redacted] ✓

We will receive an Email notification upon the detection of unusual database activities.

The Email will give the information on the suspicious security event, including the nature of the anomalous activities, database name, Server name and the event time.