Azure SQL Database disaster recovery guidance

Last updated by | Holger Linke | Mar 1, 2023 at 5:34 AM PST

Contents

- Azure SQL Database disaster recovery guidance
- Original content
  - Service outage
  - When to initiate disaster recovery during an outage
  - Outage recovery guidance
    - Planned failover (no data loss) to geo-replicated secondar...
    - Unplanned failover (potential data loss) to geo-replicated ...
    - Geo-restore
  - Configure your database after recovery
    - Update connection strings
    - Configure firewall rules
    - Configure logins and database users
    - Setup telemetry alerts
    - Enable auditing
  - Next steps

Azure SQL Database disaster recovery guidance

This is a copy of the public article Azure SQL Database disaster recovery guidance to make it findable and available in our Wiki.
Please check the original content for any changes and updates.

Original content

Azure SQL Database provides industry leading high availability guarantee of at least 99.99% to support mission critical and a wide variety of applications that need to be always available. Azure SQL Database also has capability to have turn key business continuity solution that lets you perform quick disaster recovery in the event of a regional outage. This article contains valuable information to review in advance of application deployment.

Though we continuously strive to provide high availability, there are times when Azure SQL Database service does incur outage causing unavailability of the database and thus impacting your application. When our service monitoring detects issues that cause widespread connectivity errors, failures or performance issues, the service automatically declares an outage to keep you informed.

Service outage

In the event of an Azure SQL Database service outage, you will be able to see additional details related to the outage in the following places.

- Azure portal banner

If your subscription is identified to be impacted, there will be an outage alert of a Service Issue in your Azure portal Notifications.

A screenshot from the Azure portal of a notification of an Azure SQL Database service issue.

- Help + support or Support + troubleshooting

When you create support ticket from Help + support or Support + troubleshooting, there will be information about any issues impacting your resources. Select View outage details for more information and a summary of impact. There will also be an alert in the New support request page.

A screenshot of the Help+Support page showing a notification of an active service health issue..

- Service health

The Service Health page in the Azure portal contains information about Azure data center status globally. Search for "service health" in the search bar in the Azure portal, then view Service issues in the Active events category. You can also view the health of individual resources in the Resource health page of any resource under the Help menu. A sample screenshot of the Service Health page follows, with information about an active service issue in Southeast Asia.

A screenshot of the Azure portal Service Health page during a service issue in Southeast Asia, showing the Issue and a map of affected resources.

- Email notification

If you have set up alerts, an email notification will arrive when a service outage impacts your subscription and resource. The emails arrive from "azure-noreply@microsoft.com". The body of the email would begin with "The activity log alert ... was triggered by a service issue for the Azure subscription...". For more information on service health alerts, see Receive activity log alerts on Azure service notifications using Azure portal.

When to initiate disaster recovery during an outage

In the event of a service outage impacting application resources, consider the following courses of action.

The Azure teams work diligently to restore service availability as quickly as possible but depending on the root cause it can take hours sometimes. If your application can tolerate significant downtime, you can simply wait for the recovery to complete. In this case, no action on your part is required. View the health of individual resources in the Resource health page of any resource under the Help menu. Refer to the Resource health page for updates and the latest information regarding an outage. After the recovery of the region, your application's availability is restored.

Recovery to another Azure region may require changing application connection strings or using DNS redirection, and may result in permanent data loss. Therefore, disaster recovery should be performed only when the outage duration approaches your application's recovery time objective (RTO). When the application is deployed to production, you should perform regular monitoring of the application's health and assert that the

recovery is warranted only when there is prolonged connectivity failure from the application tier to the database. Depending on your application tolerance to downtime and possible business liability, you can decide if you want to wait for service to recover or initiate disaster recovery yourself.

Outage recovery guidance

If the Azure SQL Database outage in a region hasn't been mitigated for an extended period of time and is affecting your application's service-level agreement (SLA), consider the follow these steps:

Planned failover (no data loss) to geo-replicated secondary server

If active geo-replication or auto-failover groups are enabled, check if the primary and secondary database resource status is Online in the Azure portal. If so, the data plane for both primary and secondary database is healthy. Initiate a planned failover of active geo-replication or auto-failover groups to the secondary region by using the Azure portal, T-SQL, PowerShell, or Azure CLI.

Note

> A planned failover requires full data synchronization before switching roles and does not result in data loss. Depending on the type of service outage there is no guarantee that planned failover without data loss will succeed, but it is worth trying as the first recovery option.

To initiate a planned failover, use the following links:

Technology Method Steps Active geo-replication PowerShell Failover to geo-replication secondary via PowerShell T-SQL Failover to geo-replication secondary via T-SQL Auto-failover groups Azure CLI Failover to secondary server via Azure CLI Azure portal Failover to secondary server via Azure portal PowerShell Failover to secondary server via PowerShell

Unplanned failover (potential data loss) to geo-replicated secondary server

If planned failover doesn't complete gracefully and experiences errors, or if the primary database status is not Online, carefully consider an unplanned failover with potential data loss to the secondary region.

```
Technology      Method  Steps
Active geo-replication  Azure CLI       Initiate a forced failover via Azure CLI
Azure portal    Initiate a forced failover via the Azure portal
PowerShell      Initiate a forced failover via PowerShell
T-SQL   Unplanned failover to geo-replication secondary via T-SQL
Auto-failover groups    Azure portal    Failover to secondary server via Azure portal
Azure CLI       Failover to secondary server via Azure CLI but use --allow-data-loss
PowerShell      Failover to secondary server via PowerShell but use -AllowDataLoss
```

Geo-restore

If you have not enabled active geo-replication or auto-failover groups, then as a last resort you can use geo-restore to recover from an outage. Geo-restore uses geo-replicated backups as the source. You can restore a database on any logical server in any Azure region from the most recent geo-replicated backups. You can request a geo-restore even if an outage has made the database or the entire region inaccessible.

For more information to request a geo-restore via Azure CLI, the Azure portal, PowerShell, or the REST API, see geo-restore of an Azure SQL database.

Configure your database after recovery

If you are using geo-failover or geo-restore to recover from an outage, you must make sure that the connectivity to the new database is properly configured so that the normal application function can be resumed. This is a checklist of tasks to get your recovered database production ready.

Important

> It is recommended to conduct periodic drills of your disaster recovery strategy to verify application tolerance, as well as all operational aspects of the recovery procedure. The other layers of your application infrastructure may require reconfiguration. For more information on resilient architecture steps, review the Azure SQL Database high availability and disaster recovery checklist.

Update connection strings

If you are using Active geo-replication or geo-restore, you must make sure that the connectivity to the new databases is properly configured so that the normal application function can be resumed. Because your recovered database resides in a different server, you need to update your application's connection string to point to that server. For more information about changing connection strings, see the appropriate development language for your connection library.

If you are using auto-failover groups to recover from an outage and use read-write and read-only listeners in your application connection strings, then no further action is needed as connections will be automatically directed to new primary.

Configure firewall rules

You need to make sure that the firewall rules configured on server and on the database match those that were configured on the primary server and primary database. For more information, see How to: Configure Firewall Settings (Azure SQL Database).

Configure logins and database users

Create the logins that must be present in the master database on the new primary server, and ensure these logins have appropriate permissions in the master database, if any. For more information, see Azure SQL Database security after disaster recovery.

Setup telemetry alerts

You need to make sure your existing alert rule settings are updated to map to the new primary database and the different server. For more information about database alert rules, see Receive Alert Notifications and Track Service Health.

Enable auditing

If auditing is required to access your database, you need to enable Auditing after the database recovery. For more information, see Azure SQL Auditing for Azure SQL Database.

Next steps

Review the SLA for Azure SQL Database To learn about Azure SQL Database automated backups, see SQL Database automated backups To learn about business continuity design and recovery scenarios, see Continuity

scenarios To learn about using automated backups for recovery, see restore a database from the service-initiated backups Learn more about active geo-replication Learn more about auto-failover groups Learn more about geo-restore Learn more about zone-redundant databases