

Failover group got dropped

Last updated by | Radhika Shah | Mar 20, 2023 at 3:22 PM PDT

Contents

- [Issue](#)
- [Investigation/Analysis](#)
- [Mitigation](#)
- [RCA](#)
- [Internal Reference](#)
- [Public Doc Reference](#)


Issue

Customer notices that their failover group disappeared/dropped, but claim they didn't drop it.

Investigation/Analysis

If the failover group was dropped by customer, they should be able to see it under the Activity Log on their Azure portal for as far back as 90 days. The *caller* in the json can help identify if the operation was initiated by customer. If customer is able to confirm that they didn't initiate the drop operation for the failover group, continue here with further investigation.

Run ASC troubleshooter report for Provisioning for **both** source as well as target managed instance participating in the failover group for the time period starting a few hours **before** the drop operation. Under the troubleshooter report --> Provisioning --> Operations, you can see all the operations (sorted by StartTime) that lead up to the Drop of the Failover Group.

One of scenarios that can lead to automatic drop of failover group can be due to [Inaccessible TDE protector](#) . To verify if this is case, look for the operations before the *DropManagedFailoverGroup* on the ASC troubleshooter. If the failover group was dropped due to lost access to AKV, the series of events before the drop would have operations such as *MakeManagedDbInaccessible* and *DropDatabaseCopyLink* (that is the drop for FOG link) before the *DropManagedFailoverGroup*. For example, below series of events shows up on ASC for the **target** managed instance:

originalEventTimestamp	TIMESTAMP	request_id	operation_type
2023-03-03 04:04:24.5791602	2023-03-03 04:04:41.2261982	A5537BF3-CB73-46D2-8D68-14DD71FFC08C	MakeManagedDbInaccessible
2023-03-03 04:35:02.1313442	2023-03-03 04:35:12.2826025	2285AE56-E6EB-4A5F-AEF2-A6B279DCB04E	DropDatabaseCopyLink
2023-03-03 04:35:03.4815066	2023-03-03 04:35:12.2826025	686F0BDC-6869-4E7A-B80E-C7A4B69CF812	DropDatabaseCopyLink
2023-03-03 04:35:03.6511880	2023-03-03 04:35:29.4852177	5A76DB91-C0D3-4D97-955A-176625755A35	DropDatabaseCopyLink
2023-03-03 04:35:03.6669802	2023-03-03 04:35:12.2826025	958AC706-B366-42B2-B2C9-2FC66C2AF0CE	DropDatabaseCopyLink
2023-03-03 04:35:03.6936514	2023-03-03 04:35:09.3961478	A4A303E3-65ED-4084-B6F6-E247F4BFA501	DropDatabaseCopyLink
2023-03-03 04:35:03.7611111	2023-03-03 04:35:10.4557446	B64622B3-8B45-4822-A2EC-70567F7BF86C	DropDatabaseCopyLink
2023-03-03 04:35:03.8990617	2023-03-03 04:35:09.3961478	A6B47DF6-4B24-4F69-B9F6-342FF2AC4DF3	DropDatabaseCopyLink
2023-03-03 04:35:03.9174159	2023-03-03 04:35:06.8750587	87B5295F-0F13-4A44-8ED7-CCB3EBA131F7	DropDatabaseCopyLink
2023-03-03 04:35:04.0120618	2023-03-03 04:35:12.2826025	8C1B199A-F71D-4EB2-	DropDatabaseCopyLink

originalEventTimestamp	TIMESTAMP	request_id	operation_type
		9DEF-D4A361A6700D	
2023-03-03 04:35:04.0197640	2023-03-03 04:35:29.4852177	C3DF4748-65FC-4D9E-9064-4F088E680656	DropDatabaseCopyLink
2023-03-03 04:35:04.1048847	2023-03-03 04:35:10.4557446	00C6E5CC-FC1A-47D3-8CBD-FE7F16487BFA	DropDatabaseCopyLink
2023-03-03 04:35:04.1516997	2023-03-03 04:35:12.2826025	0771F52D-AED0-4618-B8EA-366D23CFFC0C	DropDatabaseCopyLink
2023-03-03 04:35:04.2418265	2023-03-03 04:35:12.2826025	A532043F-5AA0-4DB4-8962-4C5CAE55706D	DropDatabaseCopyLink
2023-03-03 04:35:12.8163950	2023-03-03 04:35:42.2830161	2F005D3A-0165-477C-825A-2BDF6BEF69DD	DropManagedFailoverGroup

When you see the **MakeManagedDbInaccessible**, followed by the DropDatabaseCopyLink, leading to **DropManagedFailoverGroup** is a confirmation that the failover group was dropped due to Inaccessible TDE protector.

Mitigation

Customer will need to restore access to their AKV and then recreate the failover group.

RCA

RCA for why the failover group was dropped:

When TDE is configured to use a customer-managed key, continuous access to the TDE protector is required for the database to stay online. If the server loses access to the customer-managed TDE protector in AKV, in up to 10 minutes a database starts denying all connections with the corresponding error message and change its state to Inaccessible.

After access to the key is restored, taking database back online requires extra time and steps, which may vary based on the time elapsed without access to the key and the size of the data in the database:

- If key access is restored within 30 minutes, the database will autoheal within next hour.
- If key access is restored **after more than 30 minutes**, autoheal isn't possible, and bringing back the database requires extra steps on the portal and can take a significant amount of time depending on the size of the database. Once the database is back online, previously configured server-level settings such as **failover group configuration**, point-in-time-restore history, and tags **will be lost**. Therefore, it's recommended implementing a notification system that allows you to identify and address the underlying key access issues within 30 minutes.

Reference: [Inaccessible TDE protector](#) .

Internal Reference

[ICM 373491015](#) 

Public Doc Reference

[Inaccessible TDE protector](#) 