**AlwaysOn**

In this article, we are going to cover few of the Always-On issues, investigation process and the resolution steps.

Initially, AlwaysOn is basically defined using the concepts of Mirroring and Clustering concepts. The data between the Availability replicas flow in the same way as in Mirroring and the AG group failover uses the clustering technology in case of failover.

With SQL Server 2012, the supported number of Availability Replicas are five (one primary and 4 Secondary replicas) and with 2014, the number increased to nine (One Primary and Eight Secondary replicas).

**Synchronous modes:**

**Synchronous-commit Mode**: Under synchronous-commit mode, transactions wait to send the transaction confirmation to the client until the secondary replica has hardened the log to disk

**Asynchronous-commit** Mode: Under asynchronous-commit mode, the primary replica does not wait for any of the secondary replicas to harden the log. Rather, immediately after writing the log record to the local log file, the primary replica sends the transaction confirmation to the client.

**Failover Modes:**

**Automatic:** Failover automatically to other Synchronous replica which is configured for Automatic failover. Prerequisite is all the databases must be in sync with primary replica.

**Manual**: In Manual failover there are two types. One is Manual failover and other is force failover. When the availability replicas are configured with synchronous-commit mode and failed-over manually, the Ag group moves to corresponding Secondary replica. In case when secondary replica is configured for Asynchronous-commit mode, to failover to the secondary replica, this should be a force failover with data loss.

AlywaysON Issues : <https://learn.microsoft.com/en-us/troubleshoot/sql/database-engine/availability-groups/troubleshooting-log-send-queuing-in-alwayson-availability-group>

**ISSUES:**

* **Log\_reuse\_wait\_desc: AVAILABILITY\_REPLICA**

Use the below command to check the log\_reuse\_wait\_desc:

SELECT LOG\_REUSE\_WAIT\_DESC, \* FROM SYS.DATABASES

Connect to all the secondary replicas and check the state of the database.

If the database state is in Not Synchronous, try to resume the data movement.

If the database state is “Not Synchronizing/Suspect” check the disk space where log file and data file resides. If disk space is full, inform the customer to delete any unwanted files or expand the disk space. We also can try to shrink the log files of other databases whose log files resides in the same drive.

Check if there are any blockings in the secondary replicas, if found any inform the customer to wait till the blocking clears or kill the blocking SPID.

In the worst case, suggest the customer to remove the database from AG and add the database back to AG.

Inform the customer to ensure proper log backups are happening for all the databases in AG , on regular basis.

Note: Always check SQL logs and event viewer for more details. Use xp\_readerrorlog to check the error log

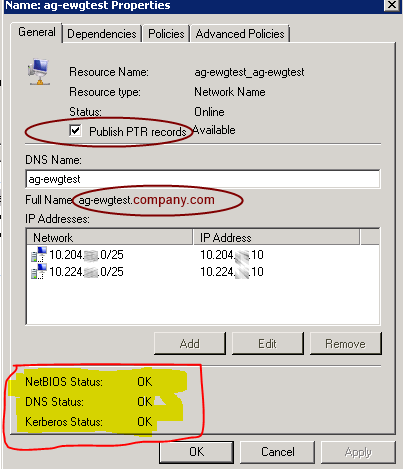
* **AG GROUP UNDER THE CLUSTER RESOURCES IS IN FAILED STATE:**

Check the status of listener IP Address. If IP Address is offline check with server team to bring the IP Address online.

Check the cluster service is running fine on all the nodes.

Always make sure it is recommended to failover the Ag group using SSMS. If AG group is failed over between Synchronous-commit replica and Asynchronous-commit replica, using the cluster manager(CLUADMIN), the AG group goes to failed state. This should be a force failover between synchronous-commit replica and asynchronous-commit replica and this force failover should be through SSMS.

Check the properties of AG group name and listener name and the status should be as in below screenshot



Check the dependencies of the Ag group. Preferred and possible owners of the AG group

Note: Always check SQL logs and event viewer for more details. Use xp\_readerrorlog to check the error log

* **AG GROUP UNDER THE SSMS IN RESOLVING MODE**

Check the SQL services are running fine on all the secondary replicas.

Check the state of AG group under the cluster resources.

Check the port 5022 is listening. Check the port 5022 is enabled in firewall on all the replicas

Check the service account has permissions on endpoint. Use the below command to grant permission.

GRANT CONNECT on ENDPOINT :: <endpoint\_name> to <service\_account>

Use the below command to check the state of endpoint.

select r.replica\_server\_name, r.endpoint\_url,

rs.connected\_state\_desc, rs.last\_connect\_error\_description,

rs.last\_connect\_error\_number, rs.last\_connect\_error\_timestamp

from sys.dm\_hadr\_availability\_replica\_states rs join sys.availability\_replicas r

on rs.replica\_id=r.replica\_id

where rs.is\_local=1

Check both the endpoints are using the same encryption algorithm

Check with customer, whether the service account password is changed recently and not updated under the SQL Server configuration Manager.

Check ‘NT Authority\SYSTEM’ is enabled and has sysadmin rights on all the replicas

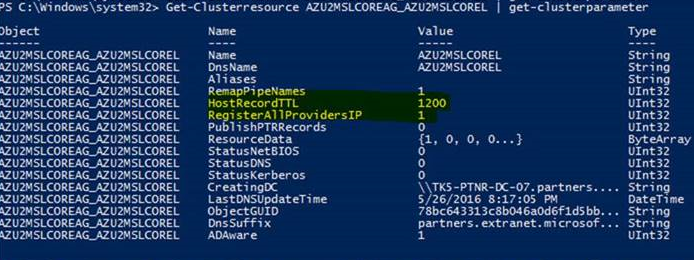
Note: Always check SQL logs and event viewer for more details. Use xp\_readerrorlog to check the error log

* **Not able to access using Listener Name:**

Check the state of IP Address is online. If IP address is offline work with server team to resolve the issue

Check whether it is Azure related or Non-Azure

In case of NonAzure, check whether all the availability replicas are in single subnet or multi-subnet. In case of multi-subnet, the RegisterAllProvidesIP cluster parameter for the listener name value should be 0.



In case of single subnet, ping the listener name and check whether it is pointing to right IP Address. Try to access with IP address, with FQDN and without FQDN and check if anyone is working.

Check the portqry on listener name and port 1433.

Check with customer whether there are any recent changes.

In case of Azure, check the probe port 59999 is enabled in firewall on all the replicas.

In case of Azure, the cluster parameter probe port value for the listener IP address should be 59999

In case of AZURE ping to the listener name will get ‘Request timeout’ error

Check with VSU team for the Azure endpoint configuration settings and ILB configuration settings