Only Active Directory logins can impersonate other Active Directory logins

Last updated by | Vitor Tomaz | Feb 24, 2023 at 3:32 AM PST

Contents

Issue

The error message *Only Active Directory logins can impersonate other Active Directory logins* is thrown when the customer tries to execute a stored procedure that contains the EXECUTE AS.

Investigation/Analysis

The database is marked as Trustworthy. Also the database owner is an AAD user - this means that when the Execute As is done, it will try to create a login token from the database owner.

The user that is executing the stored procedure is non-sysadmin and is SQL authentication.

The issue is that the impersonation of AAD users is only possible by sysadmin login or an AAD user.

Mitigation

Change the database owner to a SQL login or execute procedure under sysadmin role.

Public Doc reference

Execute As

Extending Database Impersonation by Using EXECUTE AS

Internal reference

288184369

How good have you found this content?