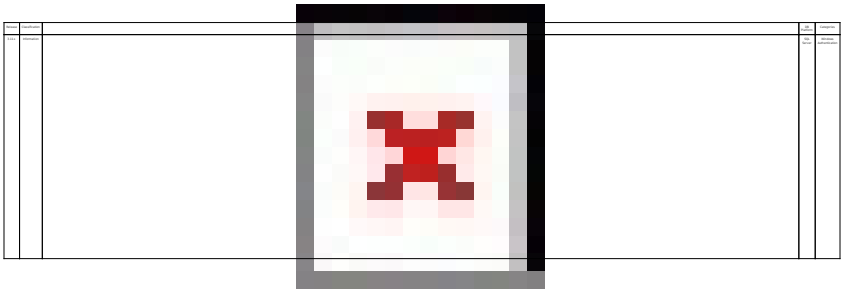
How do Authentication Offload and Windows Authentication Offload switches interact?

Ami Thakkar - 2017-08-08 - 0 Comments - in Configuration

How do Authentication Offload and Windows Authentication Offload switches

interact?



Q. How do the Authentication Offload and Windows Authentication Offload switches

interact?

ScaleArc features such as connection pooling and load balancing which require the ability to switch connections like read/write split, query level load balancing, query routing, connection migration on failures etc. require that the connection be authenticated by

ScaleArc. This can only occur if both the Authentication Offload settings are turned ON.

The Authentication Offload switch in 'Users and DB’s' is a *global* switch that turns ON/OFF the offload for all connections (regardless of the authentication mechanism requested).

The Windows Authentication Offload switch controls authentication for connections requesting Windows mechanism for offloading (for Windows machine users). When turned OFF, Authentication Offload of SQL authentication users continues to occur. This setting only applies when the global Authentication Offload switch is ON.

In older ScaleArc releases (without RODC/Kerberos authentication support), configuring a large number of users (more than 500) on a ScaleArc cluster manually was not possible because of a limitation allowing up to 500 users to be added in Users and DBs. Connections going through ScaleArc benefit from using ScaleArc caching and analytics. Turning Windows authentication offload OFF will result in situations where loadbalancing won’t work

for those connections.

If RODC or Kerberos authentication can be configured, there should be no need to turn OFF

Windows authentication offload.

Frequently asked question:

1. Why do connections for SQL auth users work when they are not added explicitly in 'Users

and DBs' whereas the same fails for Windows users ?

Authentication for Windows auth users not configured in 'Users and DBs' are dropped in ScaleArc since bypass of such connections is not possible due to the way Windows auth mechanism (NTLM) works. In NTLM, by the time the user name is known (so that we can check if it is configured on the cluster), we have already sent a ScaleArc generated NTLM challenge to the client. Now the client's auth state machine has entered a state where it can only complete the authentication with ScaleArc. So, ScaleArc cannot safely handover the authentication job to the server once it knows that it does not have the

credentials configured for the NTLM user.

Permalink:
https://support.scalearc.com/kb/articles/4282