Open in app

Jack Roper

Follow   13 Followers   About

Azure Front Door — Fun with Custom Domains, Authentication, WAFs and Load Balancing

Jack Roper   Feb 18, 2020 · 2 min read

I setup Azure app service authentication with Azure Front Door as per this article with a custom domain:

https://vincentlauzon.com/2019/07/17/azure-app-service-authentication-with-azure-front-door/

The key details to getting this working:

- leave the 'backend host header' field blank on the backend pool

- validate the custom domains on both the web app and front doors so the certificates can be created.

- Easy auth can then be turned on using a service principal.

This works nicely with one web app behind the front door.

When more than 1 web app sits behind the front door however, I was seeing the page not rendering correctly, giving different versions of the page. When using the browsers network tools, we were seeing some 302 errors returned. This is because the front door probes the web app back ends for a response, and as authentication was not turned on, these could not be reached successfully. Also when the WAF was enabled, it was blocking the attempts, showing a SQLi attack in the logs.

- A healthprobe.html file created in each web app.

- The front door load balancing setting points to /healthprobe.html

- Each web app needs a configuration value of "WEBSITE_WARMUP_PATH" added. This is the path to a file that will not be authenticated to avoid 302 errors. The value points to /healthprobe.html.

- Restart the web apps.

The front door now had a working custom domain, with multiple apps behind it and the WAF working nicely! It was authenticating for the web app with Azure easy auth whilst also allowing authentication using a service principal. Happy days!

Originally published at https://azurelynot.blogspot.com on February 18, 2020.

Azure   Azure Front Door   Azure Web App

About   Help   Legal

Get the Medium app

Download on the App Store   GET IT ON Google Play