Using CORS preflight caching with the CA API Gateway

Topic This article describes the introduction and processes of integrating CORS preflight caching with the CA API Gateway. Sample policies and documentation are attached to this issue

Solution

Background

Cross-origin resource sharing (CORS) is a mechanism that allows resources (such as fonts, images, or multimedia) on a web page to be requested from another domain outside the domain from which the resource originated. CORS defines a way in which a browser and server can interact to safely determine whether or not to allow the cross-origin request.

Open Web Application Security Project (OWASP) has identified a risk in the Cross-Origin Resource Sharing (CORS) request preflight process. Transmittal of CORS requests is handled by the client application used by the service consumer. A user could craft and send an HTTP request that does not use an allowed HTTP method or body. The CORS mechanism provides client and server applications with a protocol for engaging in a "preflight" exchange the determines what domains can request data and what HTTP methods are permitted. This exchange is typically executed using an HTTP request with the OPTIONS method. A CORS-compliant server application can respond with several CORS-specific headers that can inform the browser whether the application can request a specific resource.

The use of the preflight exchange is completely dependent upon the client application sending a preflight OPTIONS request. A client application can send an HTTP request to a service without previously sending the first request for preflight in an attempt to interact with the service and server in a malicious manner. The CORS policy implementation in the API Gateway is designed to provide a configurable proxy for web services and applications to mitigate abuse of CORS preflight processes by caching preflight requests and validating that subsequent requests correlate to an existing preflight request.

Scope

As of version 8.3.00: Formal support for CORS is not currently available as an out-of-the-box solution. The following policies have been authored by CA Services as a starting point for configuring an existing Gateway implementation to support CORS preflight request caching. Development incident SSG-8365 has been opened for this request. The policies provided in this article are only a basic example. Usage is provided with no express warranty and a Professional Services engagement will be required for further support of this implementation. If there are questions or a need to deploy CORS preflight caching then please contact CA Services via phone or email here: http://www.ca.com/us/services.aspx

Implementation

Installation notes and more detailed information with example policies can be found in the compressed archive attached to this article. Downloading and extracting the contents of the archive will provide the following items:

- *CORS Preflight Cache Service* policy
- *CORS Processor* policy
- *Example Company* policy
- *Managing CORS Preflight Scrutiny in Layer 7 Policy*

Workaround

Knowledge Base File CORS in API Gateway.zip