what is cross origin resource sharing in storagegrid

Cross-Origin Resource Sharing (CORS) in StorageGRID is a security feature that allows web applications running in one domain to access resources stored in StorageGRID buckets located in a different domain. CORS enables controlled cross-origin requests and data sharing between different domains, overcoming web browsers' same-origin policy restrictions. In StorageGRID (and similar S3-compatible object storage systems), CORS is configured at the bucket level to explicitly define which origins (domains), HTTP methods (like GET, PUT), and headers are allowed to interact with the bucket's resources.

This mechanism allows developers to build client-side web applications that can securely perform operations like authenticated GET and PUT requests on StorageGRID buckets from web pages served in other domains. When a browser makes a cross-origin request, it sends an Origin header, and StorageGRID responds with the appropriate Access-Control-Allow-Origin and related headers if the request matches the predefined CORS policy.

To set up CORS in StorageGRID, you define rules specifying:

- Allowed origins (which websites are permitted),
- Allowed HTTP methods (GET, PUT, POST, DELETE, etc.),
- Allowed headers that may be included in requests,
- Max age for caching preflight requests.

This controlled sharing ensures the security and integrity of StorageGRID resources while enabling interoperability in web environments across different origins.

In summary, CORS in StorageGRID controls and permits secure cross-domain web access to StorageGRID bucket resources, consistent with the general CORS specification used in web technologies.[1][2][3][4]