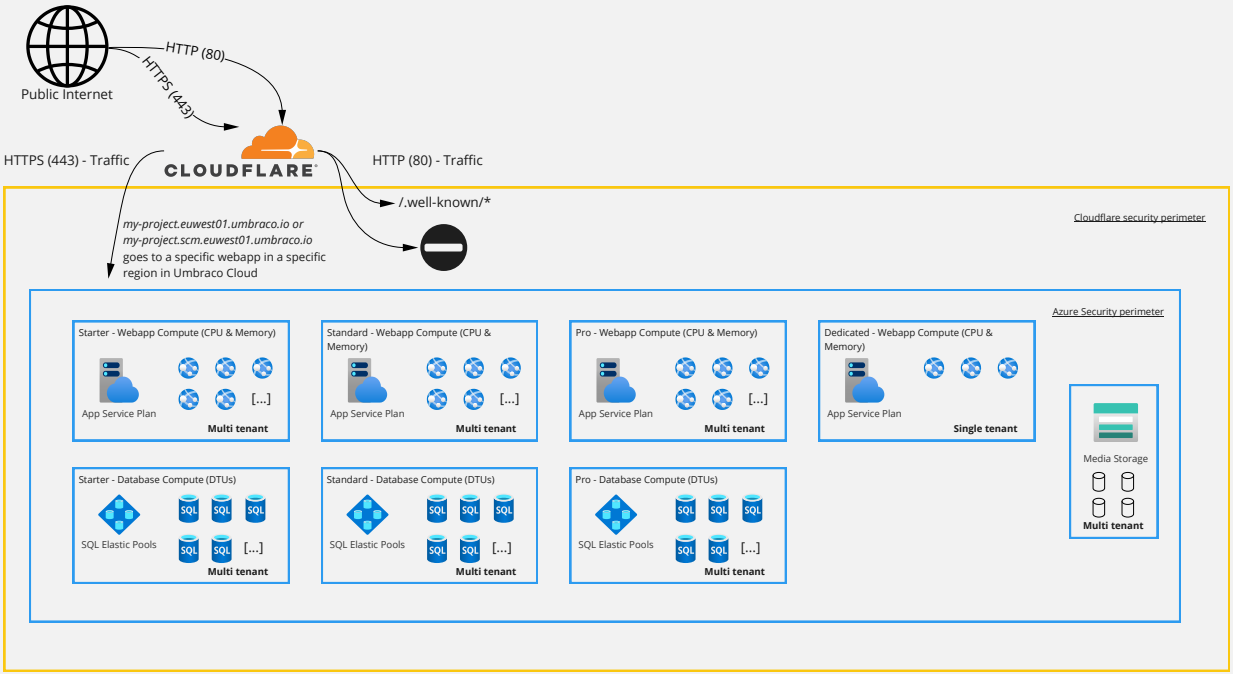
Umbraco Cloud infrastructure - security and tenancy overview



Security Details:

- DNS and CDN using Cloudflare layer 7 load balancer and DDoS protection.
- Webapps can only be accessed through Cloudflare point of entry.
- HTTPS traffic is enforced at the Cloudflare perimeter.
- Non-HTTPS traffic is only allowed to /.well-known/* for certificate validation purposes.
- A webapp cannot access other webapps running on the same compute.
- A webapp hosts a single Umbraco CMS instance.
- The file system can be accessed through the SCM hostname in a webapp hosting Umbraco CMS by authorized users signed in with Umbraco Id.
- Media library stored in Read-access geo-redundant blob storage (RA-GRS) - container isolation via SAS Tokens.
- Databases can be accessed from within Azure - firewall rules are set at the database level and blocks access from the public internet by default.
- Database servers are a logical grouping of resources - firewall rules cannot be set at the server level.
- Databases each have their own login, which is assigned per webapp.
- In Umbraco Cloud it is possible to access a database for an environment (webapp) by adding an allowed IP via the Umbraco Cloud Portal.
- It is possible to share a static range of IP addresses as with other tenants in Umbraco Cloud.
- Minimum TLS version is 1.2 and TLS 1.3 is supported.

Tenancy in Umbraco Cloud:

- Starter/Standard/Pro are multitenant in terms of compute resources for both databases and webapps.
- App Service Plans contains x number of feature and live environments (webapps) depending on the Umbraco Cloud Plan (Starter/Standard/Pro).
- Dedicated Umbraco Cloud Plans do not share Compute resources with other tenants.
- Umbraco Cloud Platform services are responsible for the lifecycle management of the Compute and Storage resources of Umbraco CMS instances.
- Each webapp consists of an Umbraco CMS instance, a local git repository and an online console for browsing the wwwroot (Kudu).
- Media is stored in a regional blob storage account with private container isolation meaning that a tenant cannot browse other tenant's media.

Backup Details:

- Webapps has 30 days hourly snapshot backups, which can be restored upon request.
- Sql databases has 30 days point in time restore, which can be restored upon request.

Password Policy:

- Between 8 and 100 characters, letters, numbers, symbols are allowed.

umbraco