1. **Introduction**

The new release of My-Drive in Amazon AWS marketplace will be available from 15 February 2026.

My-Drive offers file storage and file access solutions from different locations using heterogeneous resources. It is a web-based, cross-platform, and cross-device client application. VPN or guaranteed Internet connection is NOT required. The file storage utilizes CLOUD solutions from Amazon AWS, offered for different geographic regions for greater speed. Files are stored using AWS S3 object storage technology and a private CLOUD zone. The storage and file transfer are protected using high encryption. My-Drive is implemented using Amazon AWS services as a private CLOUD hybrid software solution. It requires CLOUD resources (AWS S3) and infrastructure within the AWS data centers, such as EC2 services for VPC, EIP, and ELB. Minimal Amazon AWS interface knowledge is required ; the AWS services help pages cover the necessary information.

2. **Requirements and recommendation**

2.1. An Amazon AWS account is required. The account should be in the name of the final user (client). Navigate to https://aws.amazon.com/ and press the " Create an AWS Account " button. Next, follow the AWS website 's instructions . The requested email address can be provided by the client. A credit card is required to validate the account.
2.2. A domain name is required to be used by the software solution for its web services address. You can use a domain name that you have or buy a new one. We recommend buying a new domain name from Amazon AWS using the Route 53 AWS service page and the created account. It will be useful to have all resources at one provider. In case you use an existing domain name, check if you have access to edit DNS records for that domain (directly or through a third party).

3. **Installation**

3.1 Find My-Drive in AWS Marketplace and install the EC2 instance .
Open your Amazon AWS account : https://aws.amazon.com/
Open the AWS Marketplace and click on Discover products.
Search for My-Drive (by Q-Bis Consult).
Follow the installation from the marketplace ; a CloudFormation Template is used.
It is mandatory to set an S3 Bucket name in the installation interface.
During the installation, you will be asked to create a PEM key to access the EC2 with SSH . Create and save the file on your computer ; it will be used if you need to add features to the installation later using SSH to connect. If you have a PEM key for the same region, it can be used instead.
The CloudFormation Template will set the security access rights and the IAM role for you.
Check the new EC2 instance in the AWS console ; you can add a fixed public IP (it is not mandatory, but the public IP changes every time you stop/start your instance).

3.2 **DNS Settings**

In order to find and use your newly created web services, DNS records should be created or modified. You will need at least an A record that points to the used IP address. DNS settings interfaces will vary for different providers. The AWS Route 53 DNS manager will allow you to create an A record that maps to an AWS EC2 ELB address, which is very handy. Amazon AWS sells domain names through the AWS Route 53 service web page.

3.3. **Application Settings**

At this point , the application should be available via a web browser.
Navigate to your application settings interface:
https:<your server name> (e.g., https://my-server.ext)
The interface will use a self - signed SSL certificate at first start. You should allow access from your browser to the settings webpage; it is acceptable for the moment and the first configuration step.
The first time, you will set the instance server and the system access settings:
The page will generate a passport key.
Passport - it is used to generate internal security keys and authorization JWT keys.
The passport is linked to the used S3 bucket ; you cannot use another passport for the same S3 bucket. Save it and keep it safe in a secured location.
If this is the first server installation for the declared S3 bucket , next you will need to set the administrator password ; otherwise, you will need to enter the administrator password to log in . You will need to log in to start the web services on the EC2 server.

3.4. **Add a certified SSL**

SSL certificates are sold by different providers ; free SSLs can be created from "Let's Encrypt." Use an SSL certificate according to the implementation and your needs . ssls.com sells wildcard certificates that can be used on domains and subdomains, which can offer flexibility later.
The SSL certificate offers trust between a web browser and a web server/service. Use the My-Drive configuration to set the SSL certificate.

3.4.1. **GET an SSL Certificate**

Certified SSL certificates are a must ; without one, there will be warning screens in desktop browsers, and the web app may not work on mobile web browsers.
SSL certificate providers will use different methods to verify that you are the owner of the domain name for which you request a certificate .
The most used methods are:
- Set a DNS record as instructed to certify you own the domain name.
- Receive an email at one domain name's master address (webmaster ...),
which cannot be used with new domains as you do not have associated emails.
We recommend the DNS method.
https://green-lock.webdo.com is a utility provided to obtain a FREE SSL certificate issued by Let's Encrypt in a short time. It provides the DNS and FILE check methods.
The Let's Encrypt SSL certificate is offered for 90 days.

3.6.2. **Install an SSL certificate**

Use the settings web application to set your new SSL certificate. A full chain certificate and the attached key are required.
You will need to restart the web services afterward in order to use the new certificate. (Info tab)
When needed, reinstall the certificate and restart the services.
Most certificates expire in one year or less.

3.5. **Install the My-Drive Web App**
Use the settings web app, the Apps tab.
Click "Install new app" for the My-Drive web app, and use the default settings. Change the installation kit address if you would like to use another source for a customized web app.

4. **Test the installation**
The web application for file access (My-Drive) should be up and running.
One VPC server is enough for around one hundred users and average usage. Later, one instance can be upgraded for more resources.

5. **Add users to the system using the WebApp web page**
The "administrator" account is used to manage users and groups.
Improved security tip : Do not add the "administrator" account to user groups.

6. **Customize the web-app interface**
Use the web-app with the "administrator" account.
Navigate to Applications/webroot/website.
Here are the web-app pages (HTML, JS, CSS, IMGs).
You can edit text files.

7. **Technical support**
Basic technical support is offered by email to a system administrator in case there is no integrator that offers technical support or maintenance (mydrive@qbis.ro).