

My-Drive software solution implementation guide

1. Introduction

My-Drive offer file storage and file access solutions from different locations using heterogeneous resources. Web based cross platform and cross devices client application. VPN or guaranteed Internet connection are NOT required.

The file storage uses CLOUD solutions from Amazon AWS offered for different geographic regions for more speed. Files are stored using the AWS S3 object storage technology and a private CLOUD zone. The storage and the file transfer is 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 into the AWS data centers as EC2 services for VPC, EIP, ELB.

Minimal Amazon AWS interfaces knowledge is required, the AWS services help pages covers required 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 "create an AWS account" button, next follow the AWS website requests. 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 it's web services address.

You can use a domain name that you have or buy a new one.

We recommend to buy a new domain name from Amazon AWS using the Route 53 AWS service page and the created account. It will be useful next 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 (direct or by a third party).

2.3. An AWS S3 bucket

The AWS S3 bucket is a storage location. It should be created before the implementation starts. (https://www.my-drive.cloud/files/Set_the_S3.pdf)

Create a new bucket, the software solution will create related files structures into the bucket. Use the Amazon AWS S3 service page to manage the bucket. DO NOT set public access to the new bucket.

2.4. Access role (IAM)

The EC2 instances software (the web services) requires access to the created S3 bucket. In order to give access an IAM role is required.

There are two options, by security reasons:

- use the global access to the S3 policy
- create a new policy that gives access to the created bucket only (recommended)

Create an IAM role based on the S3 access policy.

Recommended option is to create an IAM policy that set access to the created S3 bucket only. Next create an IAM role based on just created policy. Doing that the installation will not interfere with whatever solutions are in place or will be implemented later.

(https://www.my-drive.cloud/files/set_IAM.pdf)

3. Implementation

3.1. Install one EC2 instance from the Marketplace

(https://www.my-drive.cloud/files/set_EC2.pdf)

Start one EC2 instance using an AMI from the Marketplace, search for “My Drive” AMI and chose the release.

It can be changed later, but in relation with estimated system usage at start, you can choose from different instances types.

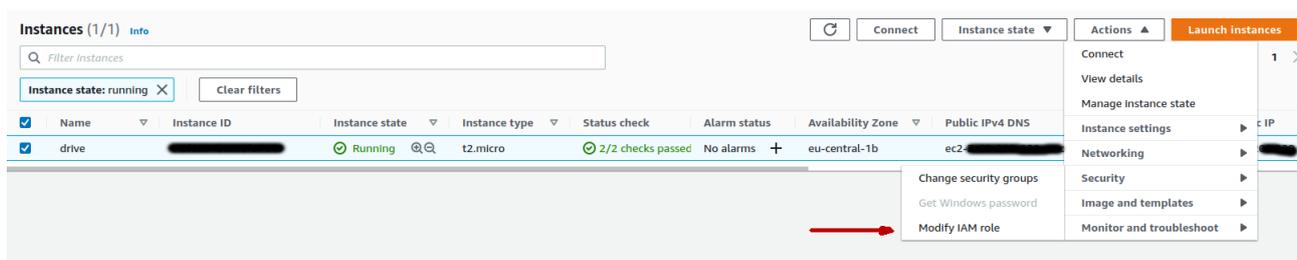
We recommend a T3a-micro for hundred users with low access, a T3a-small for hundred users with normal access and a T3a-medium for more users or high access level.

The system is scalable, more instances can work in parallel to increase the services availability.

Save and keep the created PEM access key secured all the time. It is the only way to connect to your instance later for direct console management (SSH).

Once the EC2 instance is up and running:

- use the AWS EC2 page to allocate the IAM role to the new instance. That will give access to the S3 bucket to the new instance.
- check the security group of the new instance



3.2. Security group settings: (use the AWS EC2 service interface)

The EC2 instances security groups should allow access to next ports (TCP)

- port 80 HTTP (a redirect page to the secured port)
- port 443 TCP (the application server)
- port 3200 TCP (the settings web app services)
- port 3220 TCP (the authorization web app services)
- port 22 TCP – **set filter to one IP address after installation (SSH management access)**

3.3. Add a fixed IP to the instance.

For a simple installation (without ELB balancer) a fixed IP is required.

In case your DNS are hosted by the AWS Route 53 and you are using ELB for services access balancing, a fixed IP is not required.

At first time installation, for system configuration and quick start you may start with one instance, set the system working and add scalability later.

Use AWS EC2 service page to add an EIP (elastic IP) address.

Allocate the created EIP to the EC2 instance.



3.4. DNS settings

In order to find and use your newly created web services, DNS records should be created or modified.

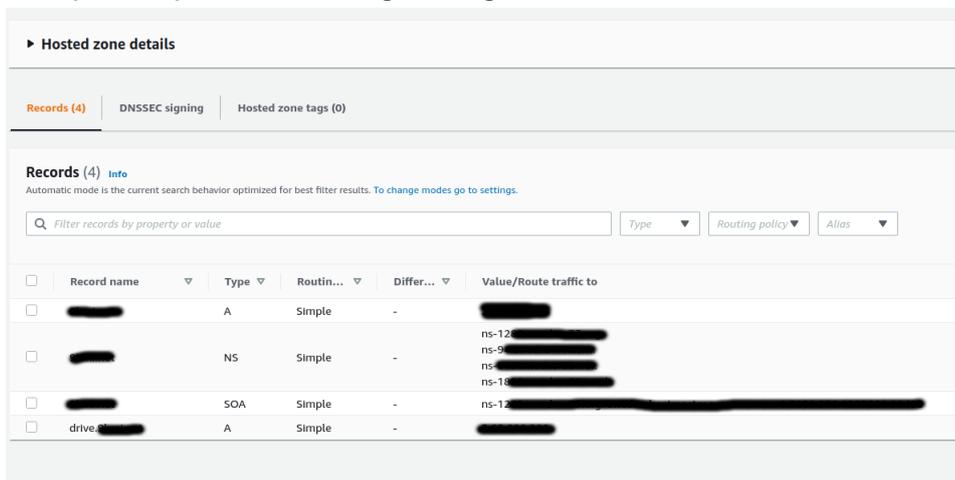
You will need at least:

An A record that point to the used IP address or a CNAME record that point to the ELB 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 an AWS EC2 ELB address which it is very handy.

Amazon AWS sell domain names thru the AWS Route 53 service web page.

Sample simple DNS settings using the Route 53 hosted zones.



drive.<domain name> is used here for the web services, A record for single EC2 installation.

The <domain name> A record is used to redirect HTTP://<domain name> requests to HTTPS://drive.<domain name>

Keep in mind that DNS settings propagation takes time. Your local system cache may store DNS requests also.

3.5. Application settings

(<https://www.my-drive.cloud/files/settings.pdf>)

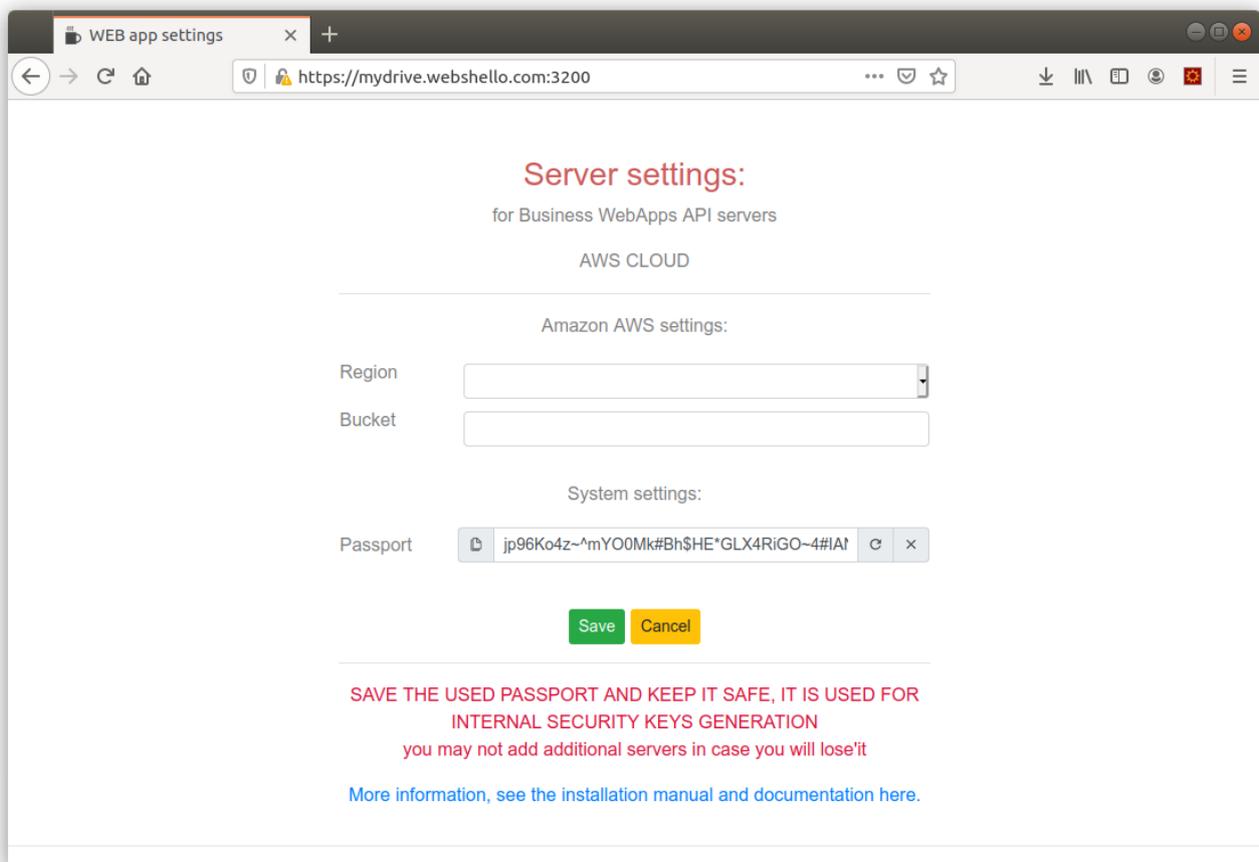
At this point the application should be available via a web browser.

Navigate to your application settings interface:

https:<your address>:3200 (Ex: <https://my-server.ext:3200>)

The interface will use a Self-Signed SSL certificate at first start. You should allow access from your browser to the settings web page, it is OK for the moment and first configuration step. If it is a second server into a servers pool the certified certificate will be loaded later, if not you will add a certified certificate to your installation later.

First time you will set the instance server and the system access settings:



Region – is the AWS region where your S3 bucket is
Bucket – the S3 bucket name

Passport – it is used to generate internal security keys and authorization JWT keys
The passport is linked to the used S3 bucket, you can not use another passport for the same S3 bucket.

If it 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 login. You will need to login in order to start the web services on the EC2 server.

3.6. Add a certified SSL

SSL certificates are sold by different providers, free SSLs can be created from “Let’s Encrypt”, use a SSL certificate according with the implementation and your needs, ssls.com sells wildcard certificates that can be used on domain and sub-domains 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 if it is the first server, each second added server will read the stored certificate from S3 CLOUD private bucket.

3.6.1. GET a SSL certificate

Certified SSL certificates are a must, without one, there will be warning screens into desktop browsers and the web app may not work on mobile web browsers.

SSL certificate providers will use different methods to check that you are the owner of the domain name you request certificate for.

Most used methods are:

- set a DNS records as instructed to certify you own the domain name
- put a text file to a specified location that can be used to download the file later (the location is under your domain name address)
- receive an email at one domain name master address (webmaster ...)

<https://green-lock.webdo.com> is a utility provided to have a FREE SSL certificate issued by Let’s Encrypt in short time. It provides the DNS and the FILE check methods.
The Let’s Encrypt SSL certificate is offered for 90 days.

See the <https://www.my-drive.cloud/services.html> web-page for recommended SSL certificate providers.

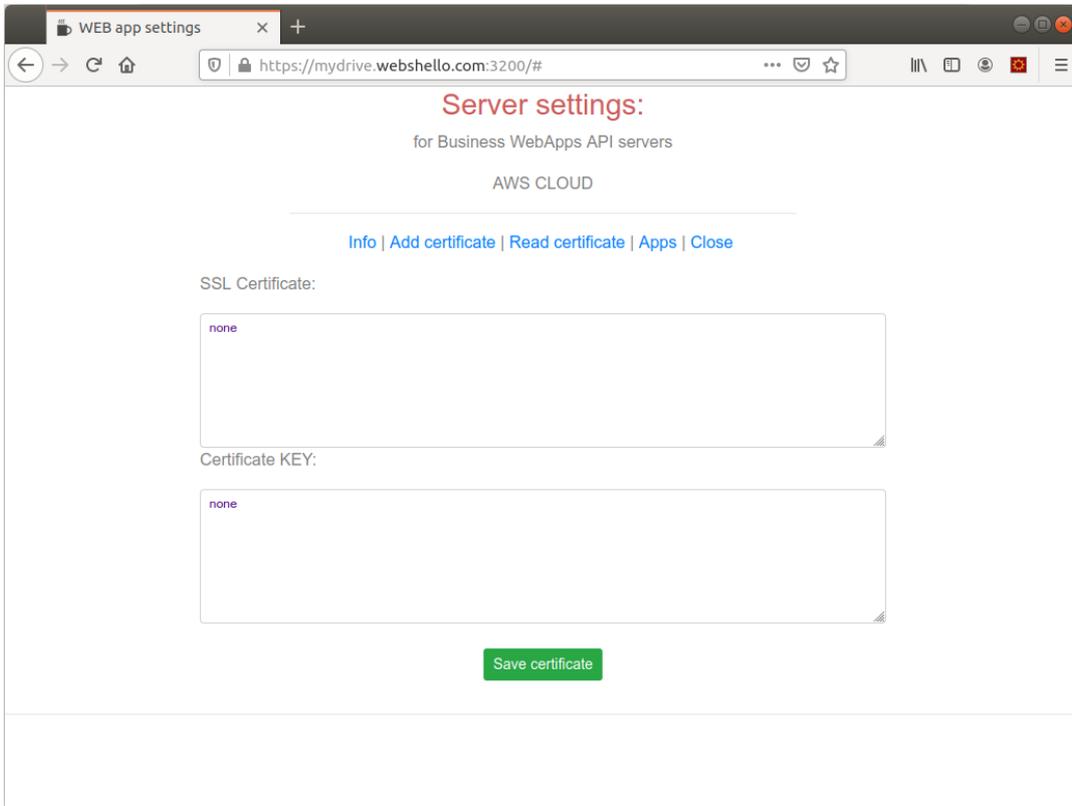
One method can be helped. In order to use the FILE verification method with the installed server, there is a running web server on port 80 that can do the service. You will need to connect to the server, more information can be found into the readme.txt file on the server (home/ubuntu/readme.txt).

Check the AWS EC2 documentation on how you can connect to a Ubuntu server instance.

3.6.2. Install a SSL certificate

Use the settings web application to set your new SSL certificate.

You will need to restart the web services after in order to use the new certificate.



The SSL certificate is the certificate and the full chains of the certificate. Check to NOT have empty lines at the beginning or the end of the entered certificate/key text. Use the “Read Certificate” tab, if your certificate is not here, check the certificate and the key, be sure no empty lines are added (top/bottom).

3.6.3. Reinstall a SSL certificate

Proceed as first time, save the new certificate with the settings web app and restart the web services.

3.7. Start the web services

Use the settings web app INFO page to see the server status. Here you can start or stop used services.

Required services are:

Services:					
Name	Id	ProcessId	Memory	CPU	
auth	3	36661	64Mb	0%	
appserver	4	39700	97Mb	0.4%	
memorydb	5	36678	63Mb	0%	
web80	6	36685	51Mb	0%	

The settings service is running by default.

The “memorydb” web services server will not start without a SSL certificate set. The services are used by the system logging.

The other services may not work as expected on mobile platforms like Android or iOS without a certified SSL certificate.

3.8. Install the My-Drive WebApp

Use the settings web app, the Apps tab

Click “Install new app”, for My-Drive web app, use the default settings. Change the installation kit address if you 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 hundred users and average usage. Later one instance can be upgraded to more resources or servers can be used in parallel (require AWS and DNS configurations for balancing).

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 users groups.

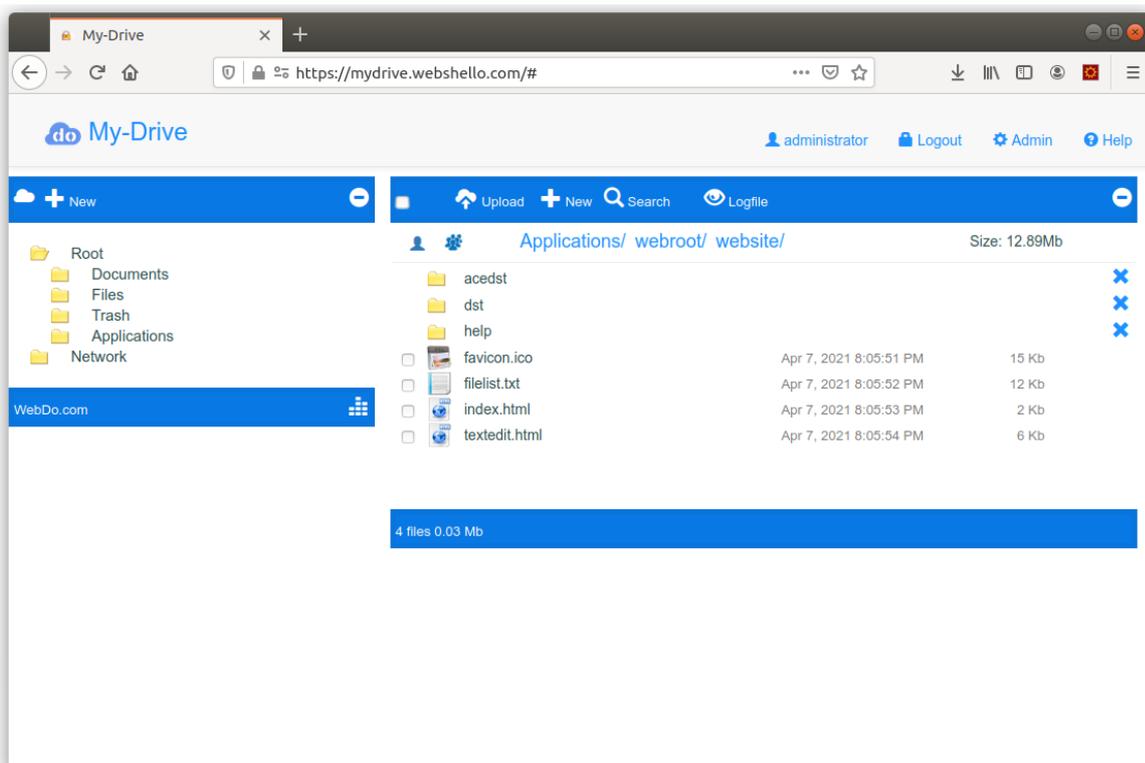
6. Customize the web-app interface

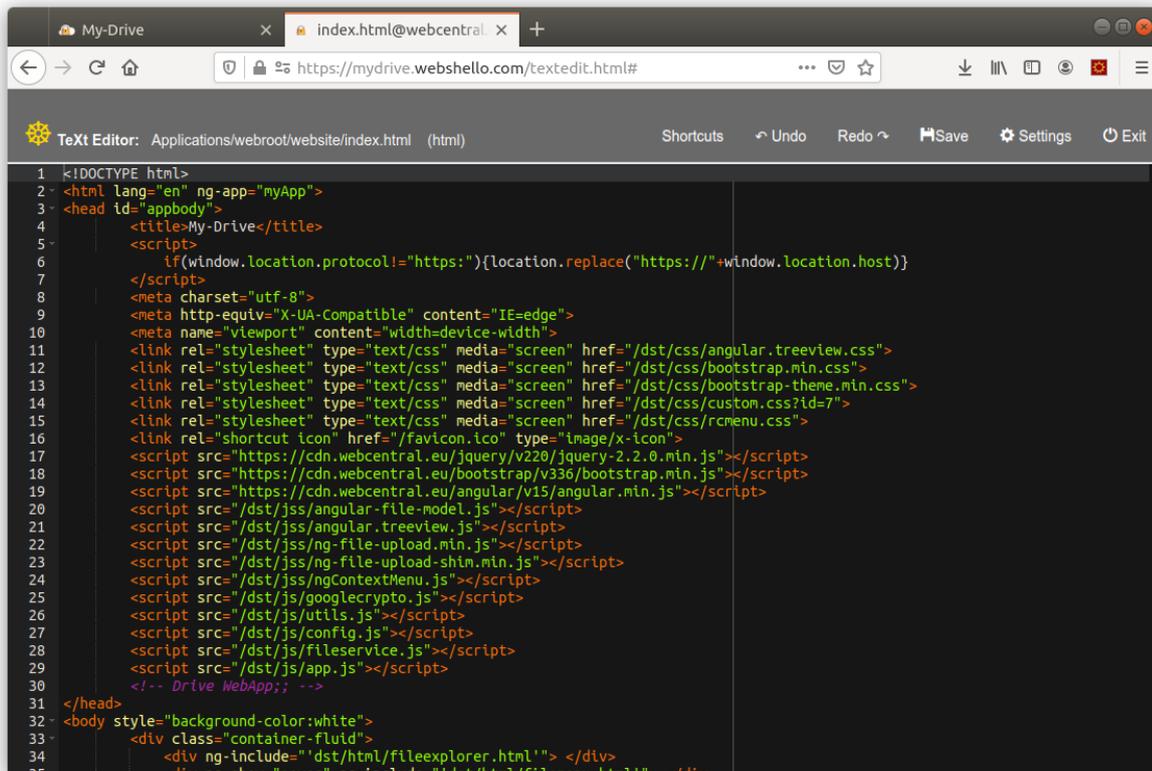
Use the web-app with the “administrator” account.

Navigate to Applications/webroot/website

Here are the web-app pages (HTML, JS, CSS, IMGs).

You can edit files using the short menu/Edit (mouse right click on files).





```
1 <!DOCTYPE html>
2 <html lang="en" ng-app="myApp">
3 <head id="appbody">
4   <title>My-Drive</title>
5   <script>
6     if(window.location.protocol!="https:"){location.replace("https://"+window.location.host)}
7   </script>
8   <meta charset="utf-8">
9   <meta http-equiv="X-UA-Compatible" content="IE=edge">
10  <meta name="viewport" content="width=device-width">
11  <link rel="stylesheet" type="text/css" media="screen" href="/dst/css/angular.treeview.css">
12  <link rel="stylesheet" type="text/css" media="screen" href="/dst/css/bootstrap.min.css">
13  <link rel="stylesheet" type="text/css" media="screen" href="/dst/css/bootstrap-theme.min.css">
14  <link rel="stylesheet" type="text/css" media="screen" href="/dst/css/custom.css?id=7">
15  <link rel="stylesheet" type="text/css" media="screen" href="/dst/css/rcmenu.css">
16  <link rel="shortcut icon" href="/favicon.ico" type="image/x-icon">
17  <script src="https://cdn.webcentral.eu/jquery/v220/jquery-2.2.0.min.js"></script>
18  <script src="https://cdn.webcentral.eu/bootstrap/v336/bootstrap.min.js"></script>
19  <script src="https://cdn.webcentral.eu/angular/v15/angular.min.js"></script>
20  <script src="/dst/js/angular-file-model.js"></script>
21  <script src="/dst/js/angular.treeview.js"></script>
22  <script src="/dst/js/ng-file-upload.min.js"></script>
23  <script src="/dst/js/ng-file-upload-shim.min.js"></script>
24  <script src="/dst/js/ngContextMenu.js"></script>
25  <script src="/dst/js/googlecrypto.js"></script>
26  <script src="/dst/js/utills.js"></script>
27  <script src="/dst/js/config.js"></script>
28  <script src="/dst/js/fileservice.js"></script>
29  <script src="/dst/js/app.js"></script>
30  <!-- Drive WebApp; -->
31 </head>
32 <body style="background-color:white">
33   <div class="container-fluid">
34     <div ng-include="dst/html/fileexplorer.html"> </div>
35     <div ng-show="cover" ng-include="dst/html/filemenu.html"> </div>
```

The browser file cache uses Etag and cache-time. Use web-page refresh to see results of your work in short time. The app is based on AngularJS framework at this time. It uses HTML5, CSS (Bootstrap 3.x), JS (AngularJS and JQuery). AngularJS is more flexible here for what it is required than Angular. Next official web app interface will be based on VueJS framework.

7. Technical support

The solution implementation may require IT and Amazon AWS knowledge, check the solution presentation web page (<https://www.my-drive.cloud/services.html>) for a solution integrator that can assist with the implementation and customization.

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)

Depending on requests complexity there can be additional fees per intervention when there is no maintenance contract. The fees level relates to complexity and confidentiality agreements required for the operation.

Being a software application solution that requires installation and implementation to the CLOUD provider with different scenarios, under a final client account, the technical support may be the subject of the implementation contract with an integrator.

Q-bis Consult present a list of software integrator on the product presentation web pages.

8. Build a scalable solution

Scalability requires installation of more VPC servers and AWS settings.

- install and configure more VPC instances, each will have access to the system configuration after initial setting.
- create and configure a balancing service using the AWS EC2 page
- add your instances to the balancer
- add listeners into the balancer for ports (80, 443, 3220).
- modify the DNS records according with the new configuration (balancer).

Ask mydrive@qbis.ro for more details and detailed instructions.

For ultra-scalable services, an auto-scaling can be used from the AWS EC2 services.

One server require settings into the Security Group. The MEMORYDB server opens port 3241 on TCP, that port should be available to all EC2 instances into the VPC.

Set next rule into the Security Group.

Custom TCP	TCP	3241	172.31.0.0/16
------------	-----	------	---------------

This rule is used to allow access to the memorydb server. The authorization service and log-file function uses the memorydb service for scalability.

Please pay attention to this rule, if it is not set correctly, the system will still work but, the authorization will be exposed to Brut-force attacks and the log-file may not work as expected.

Put the SOURCE form your VPC IPv4 CIDR.

EX: 172.31.0.0/16 is the IPv4 CIDR for current VPC

The image shows two screenshots from the AWS console. The top screenshot is the VPC Management Console for VPC ID vpc-d25de7b7, showing its IPv4 CIDR as 172.31.0.0/16. The bottom screenshot is the EC2 Management Console for Security Group ID sg-0654c, showing its name as 'sg-... - launch-wizard-1' and its inbound rules. One rule is highlighted: HTTP, TCP, Port range 80, Source 0.0.0.0/0.

