My-Drive ghid de implementare

1. Introducere

My-Drive ofera solutii pentru stocarea si partajarea fisierelor folosind resurse de tip CLOUD. Pentru access sunt folosite interfete web ce functioneaza pe sisteme de operare diferite si pe dispozitive diferite (browser web). Sistemul functioneaza fara a necesita conexiuni Internet cu trafic garantat sau solutii VPN.

Sunt folosite resuse CLOUD de la Amazon AWS. Amazon ofera centre de date in diverse zone geografice pentru a avea o latenta scazuta. In Europa sunt centre de date la Frankfurt, Paris, Milano, Dublin. Pentru Romania este recomandat centrul de date din Frankfurt. Fisierele sunt stocate folosind AWS S3 object storage si o zona privata de CLOUD. Stocarea datelor si transferul acestora este protejat prin criptare la standarde inalte.

My-Drive implementeaza solutia folosind solutii hibride, infrastructura AWS EC2 pentru servicii oferite si AWS S3 CLOUD pentru stocarea fisierelor.

Sunt folosite urmatoarele servicii AWS: S3, EC2, IAM, EIP, ELB.

Pentru implementare sunt necesare cunostinte minimale privind interfetele si serviciile oferite de Amazon AWS. Paginile de documentatie oferite de AWS contin toate informatiile necessare.

2. Recomandari si elemente necesare

2.1. In mod evident este necesar un cont Amazon AWS. Contul trebuie sa fie creat in numele utilizatorului final.

Gasiti pagina https://aws.amazon.com/ si apasati "create an AWS account", urmariti cerintele din pagina de inregistrare. Adresa de email poate fi schimbata ulterior, dar este recomandat sa fie o adresa a clientului final. Este necesar un card de credit pentru validarea contului, nu se debiteaza sume initial, poate fi schimbat ulterior foarte usor.

2.2. Este necesar un nume de domeniu ce va fi folosit ca adresa pentru serviciile oferite de My Drive.

Puteti cumpara un domeniu sau puteti folosi un domeniu existent.
Recomandam achizitia unui domeniu nou din interfata Amazon AWS Route 53 folosind contul nou creat. Este util sa avem resursele la acelasi provider, Route 53 este util ulterior in cazul in care solutia trebuie sa fie scalata pe orizontala. (R53 ofera posibilitatea de a seta adresa unul balancer (ELB) la o inregistrare DNS de tip A)
In cazul in care se foloseste un domeniu achizitionat deja va trebuie acces la serviciile DNS pentru modificari.

2.3. Este necesara o zona de stocare declarata in AWS S3 “bucket”.

Este folosita interfata serviciului AWS S3 pentru a declara o zona de stocare numita “bucket”. Un nou bucket trebuie creat inainte de a trece la pasii urmatori. Acesta va fi

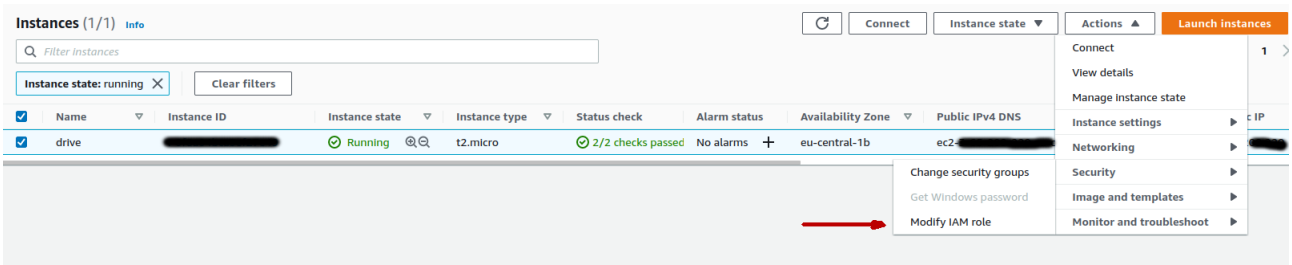
folosit pentru stocarea fisierelor si pentru informatii de configurare ce vor fi ulterior adaugate de sistem. NU setati public pentru noul bucket, de asemenea nu este necesara criptarea oferita. Sistemul implementeaza propriul model de criptare bazat pe AES256. (urmariti sa fiti in regiunea/datacenterul cel mai apropiat sau cel dorit)
(https://www.my-drive.cloud/files/Set_the_S3.pdf)

2.4. IAM “Access role”

Pentru a putea accesa resurse AWS S3 (sau alt tip de resurse) folosind o instanta EC2 instalata din marketplace, este necesara setarea unui nivel de incredere. Pentru aceasta este flosit servicul AWS IAM. Trebuie creat un rol (IAM role) ce va fi alocat ulterior instantelor EC2 folosite pentru servicii de catre My Drive.
Sunt doua optiuni:
- alocati access total la serviciile S3 unui rol (folositi regula predefinita de acces la S3)
- creati o regula (policy) de access la un singur bucket si alocati aceasta regula unui rol.
Creati un rol IAM pe baza unei regulii de acces la S3 ce acopera buckul creat anterior (global sau punctual).
Recomandam crearea unei reguli de acces pe bucket si utilizarea acesteia pentru a crea rolul IAM, in acest mod implementarea My Drive nu poate interfera cu alte solutii implementate. (https://www.my-drive.cloud/files/set_IAM.pdf)

3. Implementare

3.1. Instalati o instanta EC2 din AWS Marketplace.
(https://www.my-drive.cloud/files/set_EC2.pdf)
Folositi interfata pentru serviciul EC2 (urmariti sa fiti in regiunea/datacenterul cel mai apropiat sau cel dorit).
Lansati o instanta noua, alegeti AWS Marketplace si cautati “My Drive”.
Alegeti tipul instantei EC2, respectiv nivelul de echipare a masinii virtuale setate EC2. Poate fi modifcat mai tarziu. Recomandam o instanta de tip T micro (T3a-micro) pentru o utilizare lejera si un numar realtiv mic de utilizatori (in jur de o suta), o instanta T small (T3a-small) pentru un nivel mai mare de utilizare sau o instanta T medium (T3a-medium) pentru un nivel ridicat de utilizare. Sistemul este scalabil, in cazul in care o singura instanta nu este suficienta, mai multe instante EC2 pot functiona in paralel pentru a mari disponibilitatea sistemului (balansarea cererilor).
La instalarea unei instante EC2 se creeaza (daca nu exista deja) o cheie PEM, salvati aceasta cheie intr-un loc sigur, este folosita pentru a putea accesa direct statia Ubuntu nou creata (SSH).
Dupa ce instanta creata functioneaza:
- folositi pagina AWS EC2 pentru a aloca rolul IAM creat noii instante EC2, va fi alocat dreptul de acces la bucketul creat anterior.
- verificati grupul de securitate al instantei create

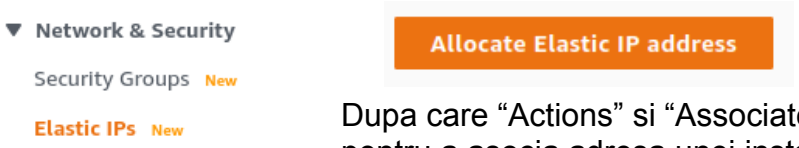


3.2. Setati grupul de securitate: (folositi interfata oferita de AWS pentru serviciul EC2)

Grupul de securitate foosit pentru instanta creata (la instalare se aloca automat) trebuie sa ofere acces la urmatoarele porturi:
- port 80 HTTP (pagina web ce este folosita pentru redirect la un port sigur - https)
- port 443 TCP (port folosit de serverul de aplicatii - https)
- port 3200 TCP (port folosit de aplicatia de configurare - https)
- port 3220 TCP (port folosit de serviciul de autorizare - https)
- port 22 TCP – setati accesul de pe IP-uri sigure (SSH acces pentru gestiune)

3.3. Adaugati o adresa IP publica fixa

Pentru o instalare simpla in care nu folositi balansarea oferita de ELB este necesar un IP fix. In general IP-ul unei instante EC2 se schimba la fiecare restart.
In cazul in care este folosit ELB si Route 53 pentru DNS nu sunt necesare IP-uri fixe.
La prima instalare, pentru configurarea sistemului incepeti cu o singura instanta si adaugati scalabilitate mai tarziu daca este cazul.
Folositi pagina AWS EC2 pentru a adauga o adresa IP fixa (EIP), alocati adresa creata instantei EC2.

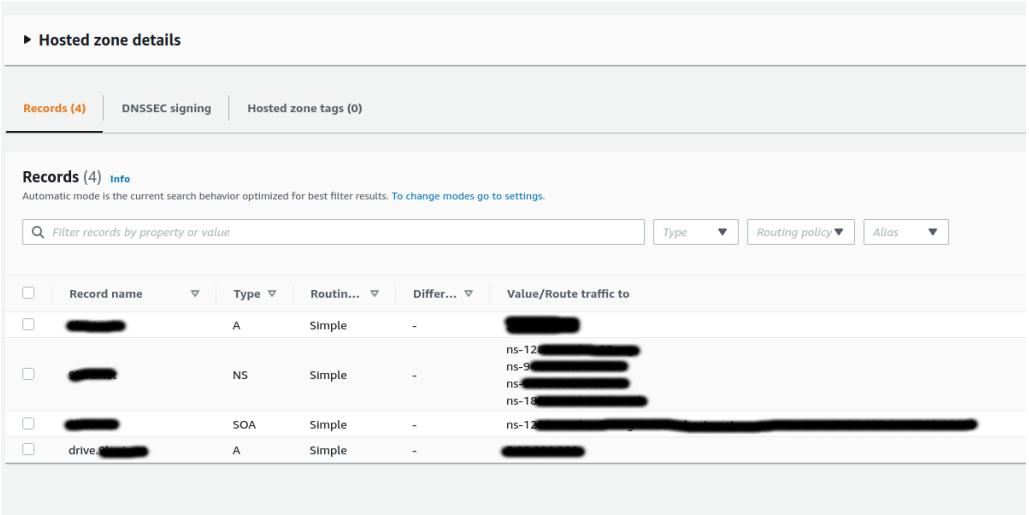


Dupa care “Actions” si “Associate Elastic IP address” pentru a asocia adresa unei instante EC2

3.4. Setari DNS
Pentru a putea folosi serviciile oferite aveti nevoie de un nume de domeniu si setari DNS.

- O inregistrare de tip A ce trimite traficul de date catre adresa IP a instantei create
- O inregistrare CNAME ce trimite traficul la adresa unui ELB (balansare)

Interfetele de editare DNS difera functie de implementare. AWS Route 53 ofera servicii DNS prin “hosted zones”. In plus Route 53 ofera suport pentru a aloca adresa unui serviciu ELB catre o inregistrare de tip A.
Amazon vinde domenii prin intermediul serviciului AWS Route 53.
Exemple de setari DNS folosind Route 53 hosted zones.

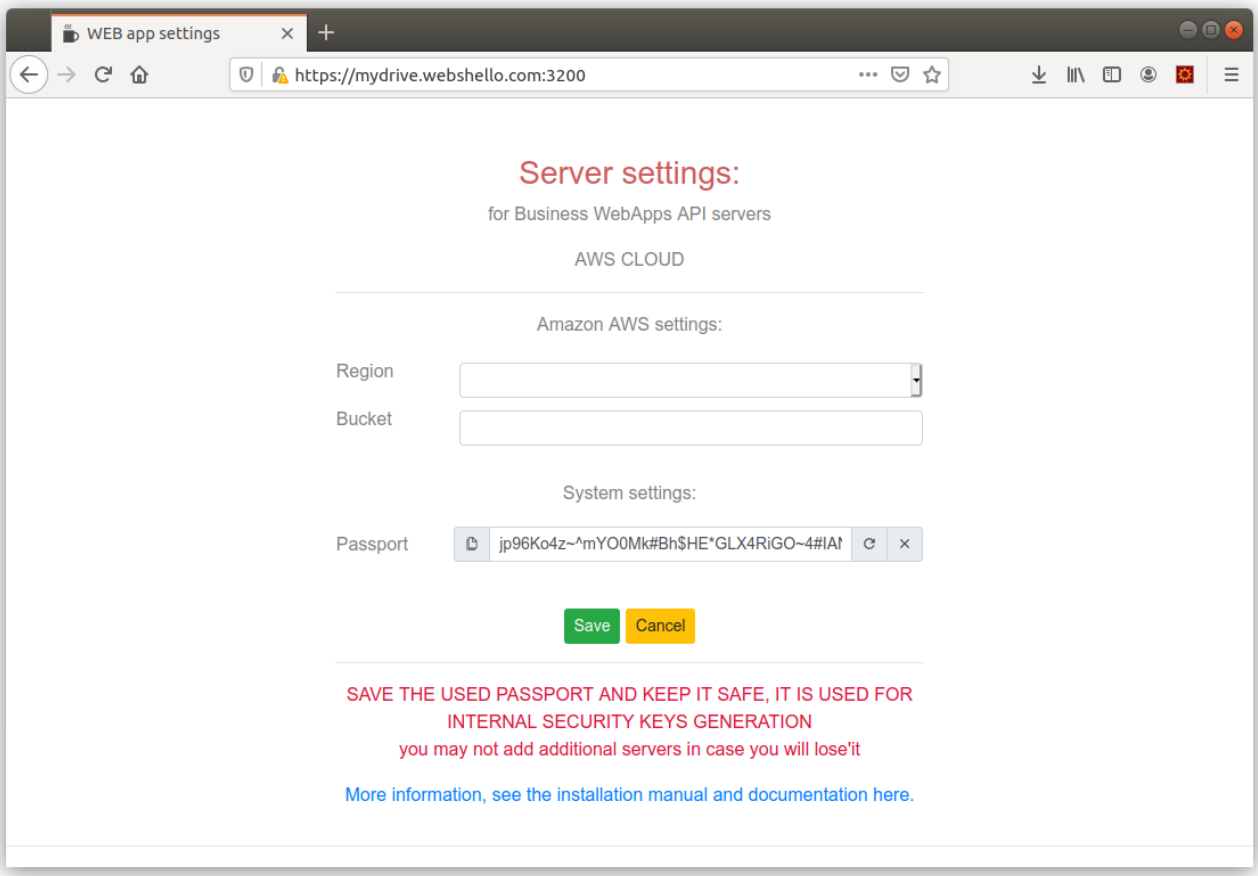


In exemplul de mai sus:
drive.<domain name> este folosit pentru serviciile web oferite, tip A pentru o singura instanta EC2 instalata.
<domain name> inregistrare tip A este folosita pentru a redirecta traficul de pe portul 80 de la adresa de domeniu la adresa subdomeniului folosit.
Setarile DNS pot fi diferite functie de implementare.

3.5. Aplicatia de configurare
(https://www.my-drive.cloud/files/settings.pdf)
In acest moment trebuie sa puteti accesa interfata de configurare a sistemului folosind un browser web.
Adresa este https://<adresa serverului>:3200 (ex: https://myserver.ext:3200)

Interfata foloseste un certificat SSL necertificat (self-signed) la pornire. Certificatul SSL trebuie schimbat mai tarziu. Este in regula sa deschideti pagina de configurare cu acest certificat, este creat instant la prima utilizare a serviciului si nu este folosit de nimeni. Daca este un al doilea server instalat, va primi certificatul SSL la prima restartare (dupa configurarea datelor de acces la bucket), altfel o sa configurati un certificat SSL ulterior.

Configurati accesul la resursele sistemului si instanta folosita.



Region – este regiunea (centrul de date) folosit (EX: Frankfurt)
Bucket – numele zonei de stocare folosita (bucket)

Passport – este folosita pentru a genera key de securitate folosite de sistem.
Passport este legat de bucket, nu poate fi modificat ulterior.

Salvati si pastrati cheia “passport” intr-un loc sigur.

Daca este prima instanta, trebuie sa setati si o parola de administrator. Daca este o a doua instanta instalata trebuie sa introduceti parola de administrator. Trebuie sa va logati ca sa porniti serviciile de aplicatie pe statia respectiva.

3.6. Add a certified SSL

Certificatele SSL sunt vandute de terti, exista SSL gratuit oferit de “Let’s Encrypt”, folositi un certificat SSL in concordanta cu nevoile implementarii. Furnizorii de certificate vand si certificate “wildcard” ce pot fi foosite pentru un domeniu si toate subdomeniile.

Certificatele SSL ofera nivelul de incredere intre un browser web si serviciile oferite.

Folositi aplicatia de configurare pentru a seta un certificat SSL daca este primul server instalat, serverele instalate ulterior vor prelua setarile din zona de stocare date S3 bucket.

3.6.1. Obtineti un certifciat SSL

Certificatele SSL asigura criptarea prin metoada utilizarii de chei publice si private.

Certificatele SSL certificate sunt absolut necesare, fara o certificare vor fi mesaje de atentionare cu privire la utilizarea de certificare neautorizate, de asemena aplicatiile pot da erori pe anumite browsere in special pe dispozitve mobile.

In momentul achizitiei unui certificat SSL sunt diferite metode prin care autoritatea emitenta (CA) verifica drepturile asupra numelui de domeniu, nume de domeniu folosit la emiterea certificatului SSL.

Cele mai folosite metode sunt:
- setati o inregistrare DNS conform specificatiilor primite (TXT)
- copiati un fisier intr-o locatie accesibila pe Interent (specificatii de la furnizor)
- confirmati un email (o adresa de tip webmaster sau administrator @ nume domeniu)

https://green-lock.webdo.com este un utilitar ce va ofera obtinerea unui certificat SSL gratuit emis de Let’s Encrypt. Foloseste metoda setarii de DNS si metoda verificarii existentei unui fisier pentru a valida accesul la un nume de domeniu. Certificatele emise de Let’s Encrypt sunt valabile 90 zile.

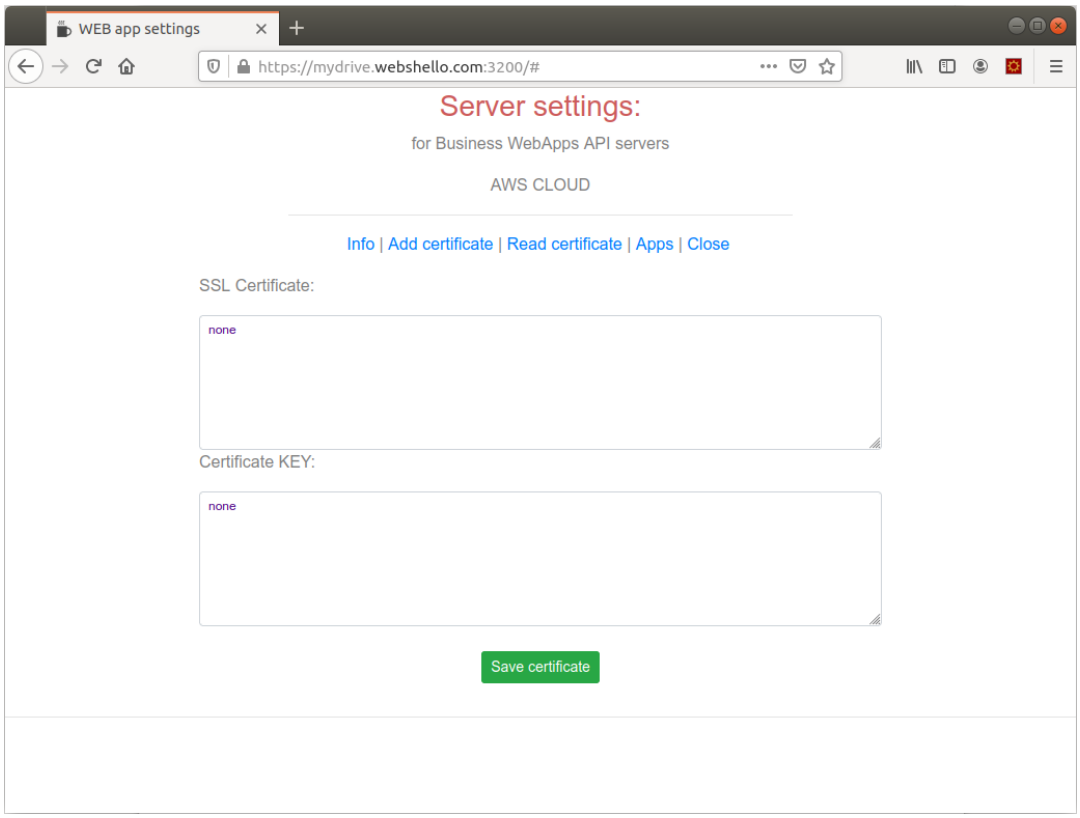
Verificati pagina https://romania.my-drive.cloud/services.html pentru recomandari privind alegerea unui provider de certificate SSL.

Una dintre metodele de verificare este suportata in mod direct de My Drive. Metoda de verificare prin fisier, Implementarea de My Drive ofera un server WEB ce ruleaza pe portul 80, acesta poate fi folosit pentru a livra un fisier cerut pe Internet. Pentru a folosi pentru prima data aceasta optiune este nevoie sa va conectati la serverul EC2 si sa urmariti instructiunile din fisierul readme.txt disponibil pe instanta de server.
(home/ubuntu/readme.txt)
Verificati documentatia AWS EC2 pentru modul de acces la un server Ubuntu prin SSH.

Ulterior, dupa ce sistemul este deja in functiune puteti seta fisierul dorit folosind interfata My Drive si contul de administrator. Fisierul de verificare trebuie salvat in: Applications/webroot/website/<cale specificata de furnizor>.

3.6.2. Instalati certificatul SSL

Folositi aplicatia de configurare pentru a seta noul certificat SSL. Este necesar sa reporniti serrviciile web ulterior (in cazul unei resetari de certificat).

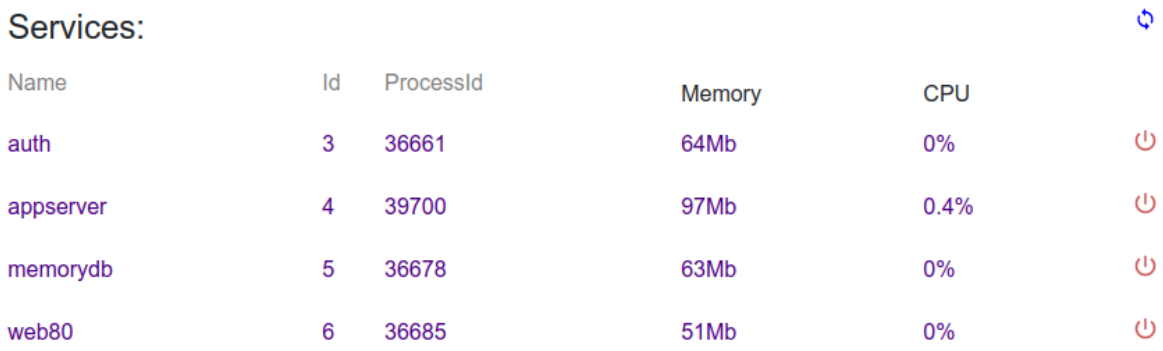


Certificatul SSL este format din certificatul domeniului si din certificatele de validare ale emitentului. In acelasi text PEM, primul este certificatul domeniului urmand certificatele inlantuite. Verificati sa nu existe linii de text goale.

Verificati certificatul instalat in tabul “Read Certificate”. Daca nu este setat corect nu o sa apara informatiile certificatului, in acest caz verificati certificatul si cheia sa fie in format corect.

3.6.3. Reinstalati un certificat SSL

Furnizorul de certificate o sa va avertizeze pe email inainte de expirarea unui certificat pentru a-l reface.
Procedati ca la pasul anterior pentru a crea si a adauga certificatul SSL, restartati serviciile WEB dupa aceea.



Serviciile pentru aplicatia de configurare ruleaza implicit.

Serviciile oferite de "memorydb" nu pornesc fara un certificat SSL setat. Acest serviciu este folosit pentru crearea de loguri.

Celelalte servicii (auth, appserver) este posibil sa nu functioneze corect fara un certificat SSL emis de o autoritate agreata CA.

3.7. Instalati aplicatia WEB My Drive

Folositi aplicatia pentru configurare, alegeti "Apps", clic pe "Install new app".

Schimbati adresa kitului de instalare daca doriti utilizarea unei alte surse pentru o aplicatie modificata.

4. Verificati instalarea curenta

Serviciile pentru aplicatia web trebuie sa fie pornite, aplicatia web poate fi lansata de la: https://<my address>

O singura instanta EC2 este suficienta pentru o suta de utilizatori in functie de nivelul de incarcare si de tipul instantei. Poate fi creata ulterior o solutie scalabila prin balansarea resurseleor intre mai multe instante EC2.

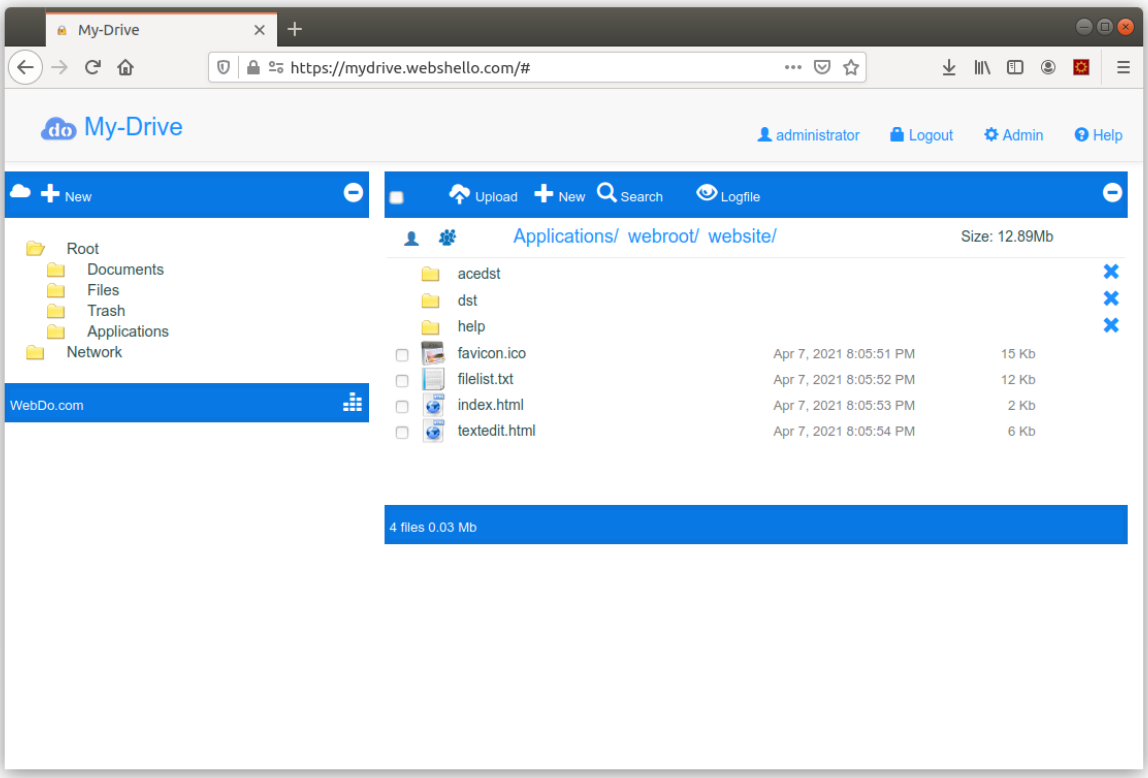
5. Adaugati utilizatori folosind interfata web

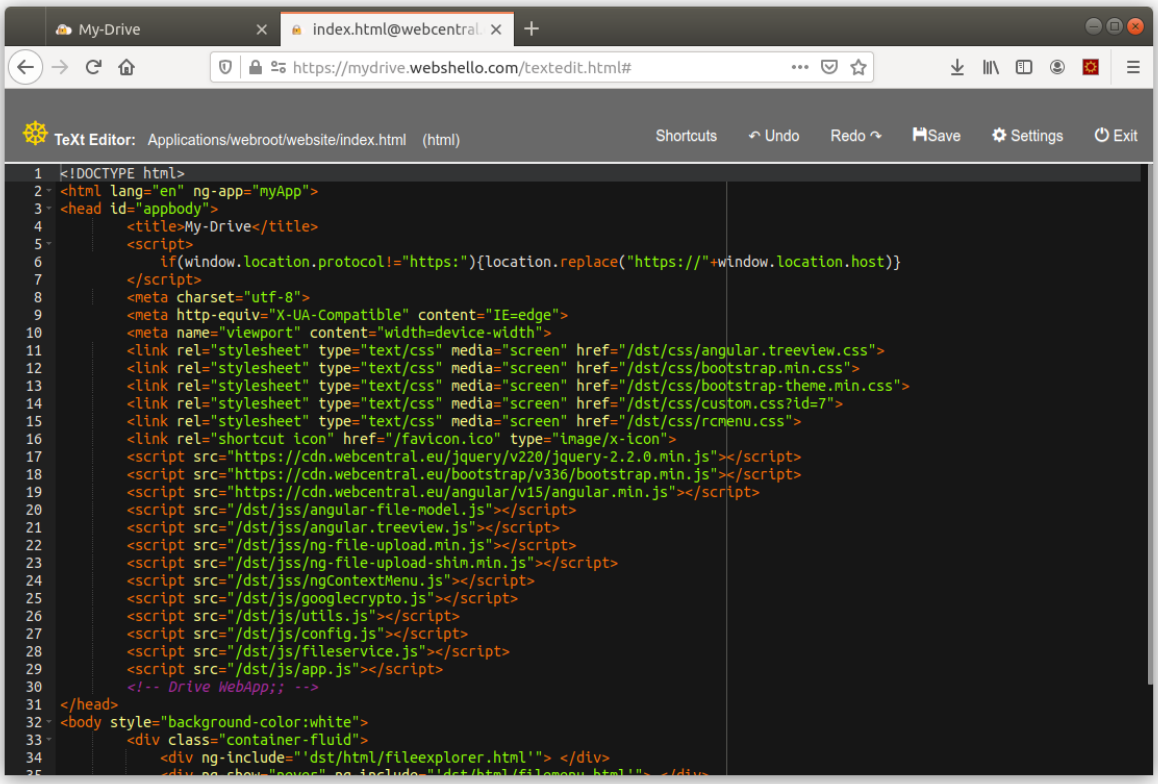
Contul "administrator" este folosit pentru a adauga utilizatori si grupuri de utilizatori. Nu este recomandat sa adaugati utilizatorul "administator" in grupuri de utilizatori.

6. Modificati interfata WEB (aplicatia web My Drive)

Folositi aplicatia WEB si contul "administrator", gasiti dosarul "Applications/webroot/ website" , aici sunt fisierele ce formeaza aplicatia web.

Puteti edita fisierele HTML, CSS si SJ (clic dreapta si EDIT pe fisiere).





Broserul web foloseste ETAG si “cache time”. Actulizati pagina web (F5 sau CTRL+R sau SHIFT+CTRL+R) pentru a reincarca o pagina WEB cu ultima versiune, altfel versiune o sa fie actualizata in minim 6 minute la o noua incarcare.
Este folosit HTM5, CSS (Bootstrap 4.7), JS (AngularJS si Jquery).

AngularJS este mai flexibil pentru acest tip de aplicatie decat Angular (poate fi modificat cu instrumente simple si nu necesita compilari de fisiere JS/CSS/HTML). Urmatoarea versiune a aplicatiei web probabil o sa fie rescrisa folosind VueJS.

7. Suport tehnic

Implementarea MY Drive necesita cunostinte tehnice IT precum si cunostinte privind utilizarea serviciilor si interfetelor Amazon AWS. Puteti gasi suport tehnic pentru implmentare in pagina https://romania.my-drive.cloud , sectiunea “Integratori”, aici este o lista de firme sau persoane ce pot oferi asistenta la implementare.

Suport tehnic de baza este oferit unui administrator de sistem in situatia in care nu sunt folosite resursele unui integrator. Cereti suport la mydrive@qbis.ro.

In functie de complexitatea cererilor pot fi taxe pentru interventii de suport tehnic atunci cand nu exista un contract de servicii de mentenanta. Taxele sunt in functie de complexitate si de nivelul de acces la date confidentiale necesar operatiilor pentru care se solictia suport tehnic.

Fiind vorba de o solutie ce necesita implementare pe un cont propriu si tinand cont de modul de implementare ce difera de la instalari simple la solutii ultrascalabile, suportul tehnic poate fi subiectul unui contract de mentenanta si suport cu un integrator.

8. Construiti o solutie scalabila

Scalabilitatea necesita utilizarea mai multor instante EC2 in paralel. Utilizarea de servicii de tip “serverless” presupune latente mari la accesarea serviciilor, din acest motiv solutia optima este utilizarea de instante EC2 ce raspund mult mai repede cu costuri rezonabile.

- instalati si configurati mai multe instante EC2
- creati si configurati un serviciu de balansare folosind AWS EC2 ELB – pagina web a serviciului.
- adaugati instantele la serviciul ELB nou creat
- adaugati rute “listeners” in serviciul de balansare pentru porturile (80, 443 si 3220)
- modificati inregistrarile DNS pentru a utiliza adresa serviciului de balansare (ELB) creat.

Ne puteti consulta pentru detalii privind implementari specifice la mydrive@qbis.ro.
Pentru solutii ultrascalabile poate fi folosit serviciul de scalare automata impreuna cu serviciul de balansare ELB prin monitorizarea incarcarii la un moment dat.

Un anumit serviciu necesita setari in grupul de securitate. Serviciul MEMORYDB deschide portul 3241 ce este disponibil doar in grupul de instante VPC. Acest port trebuie sa poata fi accesat de toate instantele din grup.

Setati urmatoarea regula in grupul de securitate: (Exemplu)

Custom TCP	TCP	3241	172.31.0.0/16

Aceasta regula este folosita pentru a acorda acces tuturor instantelor la serviciile oferite la un moment dat de unul din servere pentru MEMORYDB. Acest serviciu este utilizat pentru a verifica autorizarea si pentru fisiere de log.

Verificati cu atentie aceasta regula, daca nu este setata corect, sistemul functioneaza cu limitari, respectiv nu va putea respinge atacuri de tip “brut-force” la autorizare iar inregistrarea logurilor nu va avea acuratete (lipsa informatii).

Sursa pentru aceasta regula trebuie sa fie IPv4 CIDR al grupului de instante EC2 curent (VPC). EX: 172.31.0.0/16 este IPv4 CIDR pentru VPC curent, aceasta inforrmatie difera de la VPC la VPC.

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