Rapport du Projet 1 - Azure

1. Le nom des coéquipiers

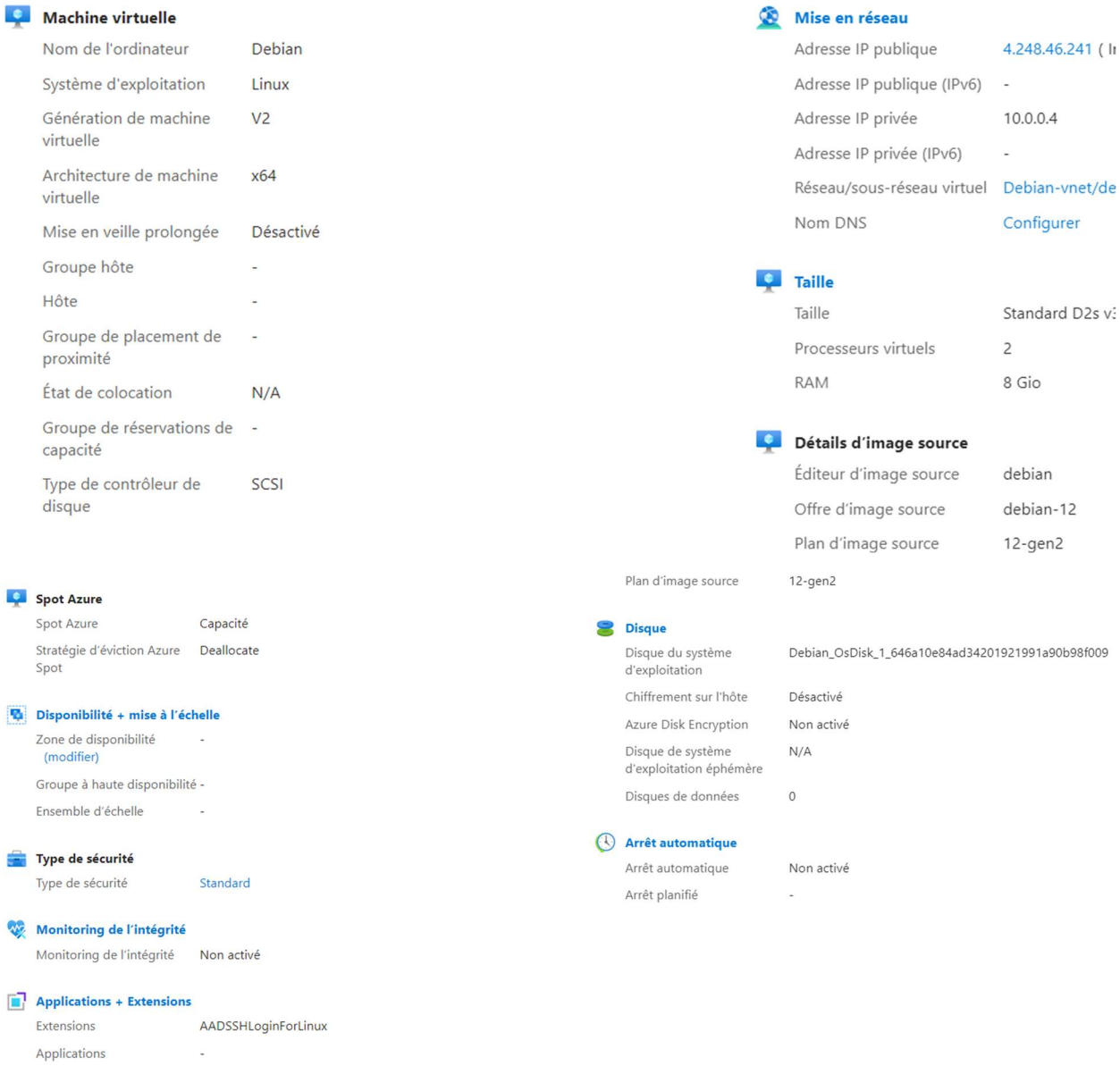
- François Joly
- Stéphane Provost

2. L'adresse IP de votre serveur ainsi que le nom de votre domaine

- Adresse IP : 4.248.46.241
- Nom de domaine : plantesvertesinc.info

3. Une description de la VM choisit

- Ressources et système d'exploitation utilisé
    - Debian 12 "Bookworm" - Génération2 X64
    - Standard D2s v3
    - 2 processeurs virtuels
    - 8 Gio de mémoire
    - SSD Standard LRS 30 Gio



Machine virtuelle

Nom de l'ordinateur	Debian
Système d'exploitation	Linux
Génération de machine virtuelle	V2
Architecture de machine virtuelle	x64
Mise en veille prolongée	Désactivé
Groupe hôte	-
Hôte	-
Groupe de placement de proximité	-
État de colocation	N/A
Groupe de réservations de capacité	-
Type de contrôleur de disque	SCSI

Mise en réseau

Adresse IP publique	4.248.46.241 (I
Adresse IP publique (IPv6)	-
Adresse IP privée	10.0.0.4
Adresse IP privée (IPv6)	-
Réseau/sous-réseau virtuel	Debian-vnet/de
Nom DNS	Configurer

Taille

Taille	Standard D2s v3
Processeurs virtuels	2
RAM	8 Gio

Détails d'image source

Éditeur d'image source	debian
Offre d'image source	debian-12
Plan d'image source	12-gen2

Spot Azure

Spot Azure	Capacité
Stratégie d'éviction Azure Spot	Deallocate

Disponibilité + mise à l'échelle

Zone de disponibilité (modifier)	-
Groupe à haute disponibilité	-
Ensemble d'échelle	-

Type de sécurité

Type de sécurité	Standard

Monitoring de l'intégrité

Monitoring de l'intégrité	Non activé

Applications + Extensions

Extensions	AADSSHLoginForLinux
Applications	-

Plan d'image source 12-gen2

Disque

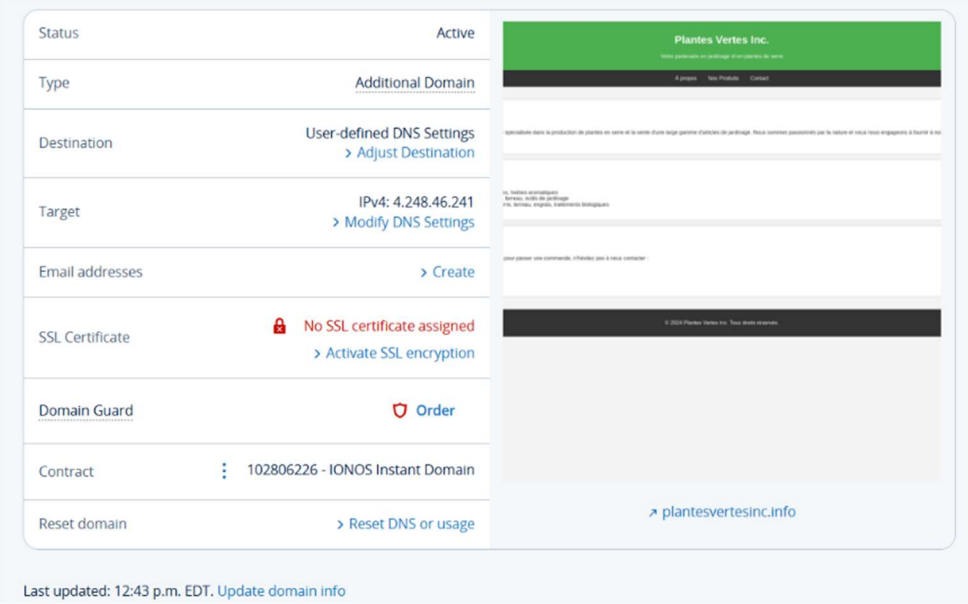
Disque du système d'exploitation	Debian_OsDisk_1_646a10e84ad34201921991a90b98f009
Chiffrement sur l'hôte	Désactivé
Azure Disk Encryption	Non activé
Disque de système d'exploitation éphémère	N/A
Disques de données	0

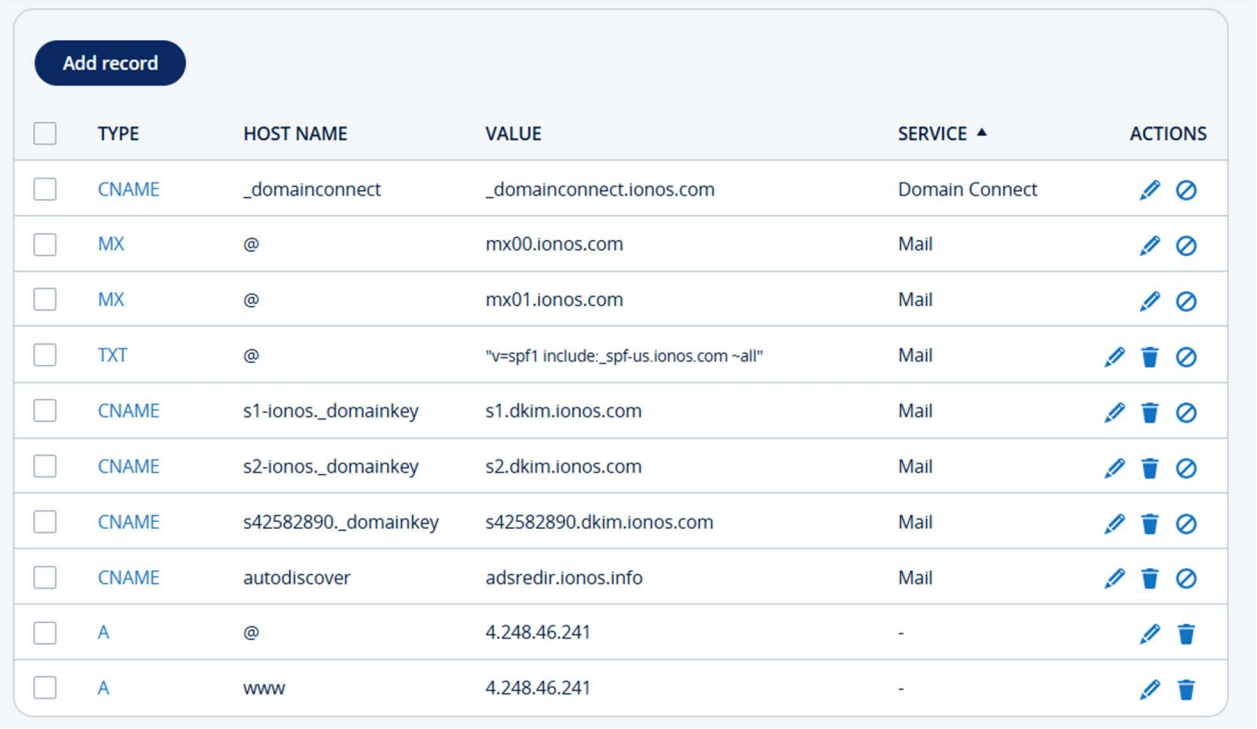
Arrêt automatique

Arrêt automatique	Non activé
Arrêt planifié	-

4. Une description des installations et des configurations

- Création du domaine plantesvertesinc.info :
  - Nous avons fait l'acquisition du nom de domaine via la plateforme IONOS. Après avoir payé les frais, nous avons changé le DNS Record pour l'adresse de notre serveur.



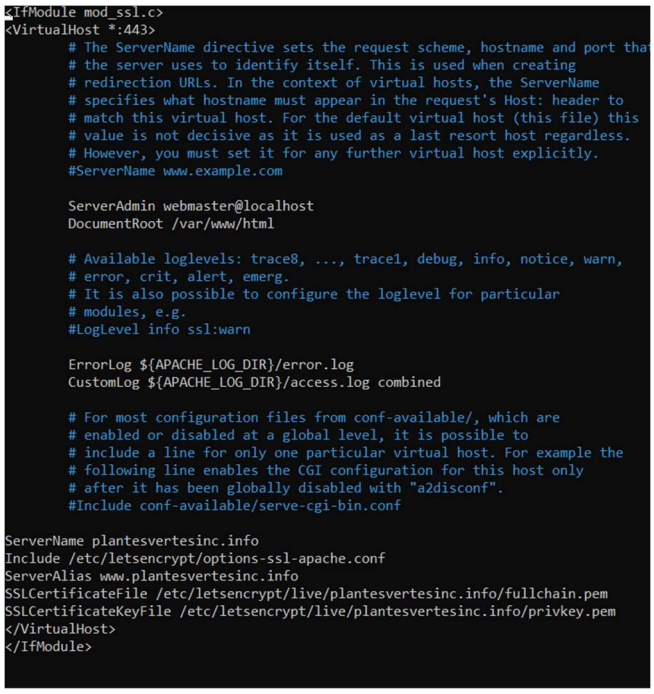


- Installation du serveur web :

Nous avons choisi d'installer Apache comme serveur web. Nous avons suivi la procédure disponible sur le site de tecmint avec succès.

https://www.tecmint.com/install-apache-with-ssl-on-debian/

- Obtention du certificat SSL :
    - Nous avons suivi la procédure de tecmint qui utilise certbot. Le tout s'effectue en quelques commandes.



```
<IfModule mod_ssl.c>
<VirtualHost *:443>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf

ServerName plantesvertesinc.info
Include /etc/letsencrypt/options-ssl-apache.conf
ServerAlias www.plantesvertesinc.info
SSLCertificateFile /etc/letsencrypt/live/plantesvertesinc.info/fullchain.pem
SSLCertificateKeyFile /etc/letsencrypt/live/plantesvertesinc.info/privkey.pem
</VirtualHost>
</IfModule>
```

    - Le résultat de la vérification qui montre le certificat en utilisation.

Lecteur du certificat : plantesvertesinc.info

Général | Détails

Émis pour

Nom commun (CN)	plantesvertesinc.info
Organisation (O)	<Ne fait pas partie du certificat>
Unité d'organisation (OU)	<Ne fait pas partie du certificat>

Émis par

Nom commun (CN)	E6
Organisation (O)	Let's Encrypt
Unité d'organisation (OU)	<Ne fait pas partie du certificat>

Durée de validité

Émis le	lundi 9 septembre 2024 à 10:24:06
Expire le	dimanche 8 décembre 2024 à 09:24:05

Empreintes SHA-256

Certificat	baefeccc97b4d599dcca1cfdff24d75624661c5bd745f739a8633d86ad6edc01
Clé publique	44607a769ca95e77408cccda123253b2cef5635dcc7a73c38ec66894c8e5e220

5. Une description de la tâche

- Installation de l'IPS Crowdsec
  https://docs.vultr.com/how-to-install-crowdsec-on-debian-11
  - Installation de l'agent à partir du repository

```
azureuser@Debian:~$ sudo curl -s https://packagecloud.io/install/repositories/crowdsec/crowdsec/script.deb.sh | sudo bash
```

```
azureuser@Debian:~$ sudo systemctl status crowdsec
● crowdsec.service - Crowdsec agent
     Loaded: loaded (/lib/systemd/system/crowdsec.service; enabled; preset: enabled)
     Active: active (running) since Mon 2024-09-09 16:19:36 UTC; 17s ago
    Process: 7259 ExecStartPre=/usr/bin/crowdsec -c /etc/crowdsec/config.yaml -t -error (code=exited, s>   Main PID: 7267 (crowdsec)
      Tasks: 8 (limit: 9517)
     Memory: 37.8M
        CPU: 3.369s
     CGroup: /system.slice/crowdsec.service
             ├─7267 /usr/bin/crowdsec -c /etc/crowdsec/config.yaml
             └─7277 journalctl --follow -n 0 _SYSTEMD_UNIT=ssh.service
```

  - Vérification de la machine surveillée

```
azureuser@Debian:~$ sudo cscli machines list
```

Name	IP Address	Last Update	Status	Version	Auth Type	Last Heartbeat
272c25abcc8e471da4876760adb319bcmRei4XHwA5upuqUj	127.0.0.1	2024-09-09T16:19:36Z	✔	v1.6.2-debian-pragmatic-amd64-16bfab86-linux	password	54s

  - Installation du bouncer

```
azureuser@Debian:~$ sudo apt install crowdsec-firewall-bouncer-iptables -y
```

```
azureuser@Debian:~$ sudo systemctl status crowdsec-firewall-bouncer.service
● crowdsec-firewall-bouncer.service - The firewall bouncer for CrowdSec
     Loaded: loaded (/etc/systemd/system/crowdsec-firewall-bouncer.service; enabled; preset: enabled)
     Active: active (running) since Mon 2024-09-09 16:21:13 UTC; 18s ago
    Process: 7538 ExecStartPre=/usr/bin/crowdsec-firewall-bouncer -c /etc/crowdsec/bouncers/crowdsec-fi>
   Main PID: 7563 (crowdsec-firewa)
      Tasks: 7 (limit: 9517)
     Memory: 8.2M
```

  - Commandes pour observer les alertes, décisions et réglages.
    - Nous pouvons voir qu'en peu de temps d'utilisation, deux adresses IP ont été bloquées.

```
azureuser@Debian:~$ sudo cscli alerts list
```

ID	value	reason	country	as	decisions	created_at
3	Ip:167.94.146.61	crowdsecurity/http-bad-user-agent	US	398705 CENSYS-ARIN-02	ban:1	2024-09-10 13:59:09.736767874 +0000 UTC
1	Ip:167.94.138.59	crowdsecurity/http-bad-user-agent	US	398324 CENSYS-ARIN-01	ban:1	2024-09-09 16:42:32.66301868 +0000 UTC

```
azureuser@Debian:~$ sudo cscli decisions list
```

ID	Source	Scope:Value	Reason	Action	Country	AS	Events	expiration	Alert ID
15002	crowdsec	Ip:167.94.146.61	crowdsecurity/http-bad-user-agent	ban	US	398705 CENSYS-ARIN-02	2	3h28m51.581996499s	3

```
azureuser@Debian:~$ sudo cscli metrics

Acquisition Metrics:
```

Source	Lines read	Lines parsed	Lines unparsed	Lines poured to bucket	Lines whitelisted
file:/var/log/apache2/access.log	25	25	-	22	-
file:/var/log/apache2/error.log	2	2	-	-	-
file:/var/log/nginx/access.log	3	3	-	2	-
journalctl:journalctl-_SYSTEMD_UNIT=ssh.service	26	7	19	22	-

Local API Alerts:

Reason	Count
crowdsecurity/http-bad-user-agent	2

Local API Decisions:

Reason	Origin	Action	Count
crowdsecurity/http-wordpress-scan	CAPI	ban	241
crowdsecurity/CVE-2017-9841	CAPI	ban	99
crowdsecurity/CVE-2019-18935	CAPI	ban	16
crowdsecurity/CVE-2023-22515	CAPI	ban	1
crowdsecurity/fortinet-cve-2018-13379	CAPI	ban	4
crowdsecurity/http-open-proxy	CAPI	ban	1297
crowdsecurity/http-sensitive-files	CAPI	ban	186
crowdsecurity/ssh-bf	CAPI	ban	2258
crowdsecurity/ssh-slow-bf	CAPI	ban	4257
crowdsecurity/CVE-2022-37042	CAPI	ban	1
crowdsecurity/apache_log4j2_cve-2021-44228	CAPI	ban	29
crowdsecurity/http-crawl-non_statics	CAPI	ban	295
crowdsecurity/http-cve-2021-41773	CAPI	ban	194
crowdsecurity/netgear_rce	CAPI	ban	40
crowdsecurity/http-admin-interface-probing	CAPI	ban	70
crowdsecurity/CVE-2022-35914	CAPI	ban	2
crowdsecurity/http-generic-bf	CAPI	ban	27
crowdsecurity/jira_cve-2021-26086	CAPI	ban	20
crowdsecurity/thinkphp-cve-2018-20062	CAPI	ban	106
crowdsecurity/CVE-2023-49103	CAPI	ban	64
crowdsecurity/ssh-cve-2024-6387	CAPI	ban	24
crowdsecurity/nginx-req-limit-exceeded	CAPI	ban	308
crowdsecurity/CVE-2022-26134	CAPI	ban	3
crowdsecurity/http-backdoors-attempts	CAPI	ban	95
crowdsecurity/http-bad-user-agent	CAPI	ban	4430
crowdsecurity/http-bad-user-agent	crowdsec	ban	1
crowdsecurity/http-cve-probing	CAPI	ban	7
crowdsecurity/http-probing	CAPI	ban	1832
crowdsecurity/f5-big-ip-cve-2020-5902	CAPI	ban	1
crowdsecurity/http-cve-2021-42013	CAPI	ban	2
crowdsecurity/http-path-traversal-probing	CAPI	ban	101
ltsich/http-w00tw00t	CAPI	ban	3

Local API Metrics:

Route	Method	Hits
/v1/alerts	GET	2
/v1/alerts	POST	1
/v1/decisions/stream	GET	788
/v1/heartbeat	GET	131
/v1/watchers/login	POST	5

Local API Bouncers Metrics:

Bouncer	Route	Method	Hits
cs-firewall-bouncer-1725898868	/v1/decisions/stream	GET	788

Local API Bouncers Metrics:

Bouncer	Route	Method	Hits
cs-firewall-bouncer-1725898868	/v1/decisions/stream	GET	788

Local API Machines Metrics:

Machine	Route	Method	Hits
272c25abcc8e471da4876760adb319bcmRei4XHwA5upuqUj	/v1/alerts	GET	2
272c25abcc8e471da4876760adb319bcmRei4XHwA5upuqUj	/v1/alerts	POST	1
272c25abcc8e471da4876760adb319bcmRei4XHwA5upuqUj	/v1/heartbeat	GET	131

Parser Metrics:

Parsers	Hits	Parsed	Unparsed
child-crowdsecurity/apache2-logs	29	27	2
child-crowdsecurity/http-logs	90	51	39
child-crowdsecurity/nginx-logs	3	3	-
child-crowdsecurity/sshd-logs	294	7	287
child-crowdsecurity/syslog-logs	26	26	-
crowdsecurity/apache2-logs	27	27	-
crowdsecurity/dateparse-enrich	37	37	-
crowdsecurity/geoip-enrich	35	35	-
crowdsecurity/http-logs	30	21	9
crowdsecurity/nginx-logs	3	3	-
crowdsecurity/non-syslog	30	30	-
crowdsecurity/sshd-logs	26	7	19
crowdsecurity/syslog-logs	26	26	-
crowdsecurity/whitelists	37	37	-

Scenario Metrics:

Scenario	Current Count	Overflows	Instantiated	Poured	Expired
crowdsecurity/http-bad-user-agent	-	1	1	2	-
crowdsecurity/http-crawl-non_statics	-	-	13	14	13
crowdsecurity/http-probing	-	-	4	6	4
crowdsecurity/http-sensitive-files	-	-	2	2	2
crowdsecurity/ssh-bf	-	-	4	7	4
crowdsecurity/ssh-bf_user-enum	-	-	4	4	4
crowdsecurity/ssh-slow-bf	-	-	4	7	4
crowdsecurity/ssh-slow-bf_user-enum	-	-	4	4	4

Whitelist Metrics:

Whitelist	Reason	Hits	Whitelisted
crowdsecurity/whitelists	private ipv4/ipv6 ip/ranges	37	-

- Tentative d'ajout d'un compteur de visite sur le site web (non complété):

```
<script src="https://cdn.commoninja.com/sdk/latest/commonninja.js" defer></script>
<div class="commonninja_component pid-14e353ad-842a-4cb8-8ab8-44d37f7331f3"></div>

<script type="text/javascript" src="http://www.websitegoodies.com/counter.php?id=75633&color="></script>
```

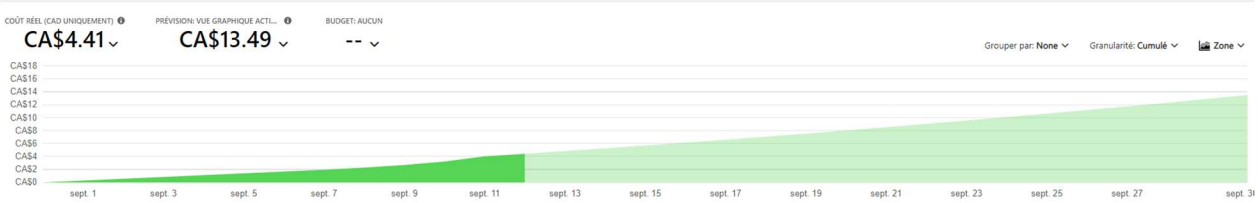
  - Preuve de fonctionnement dans un site web sous Windows :

4 Views

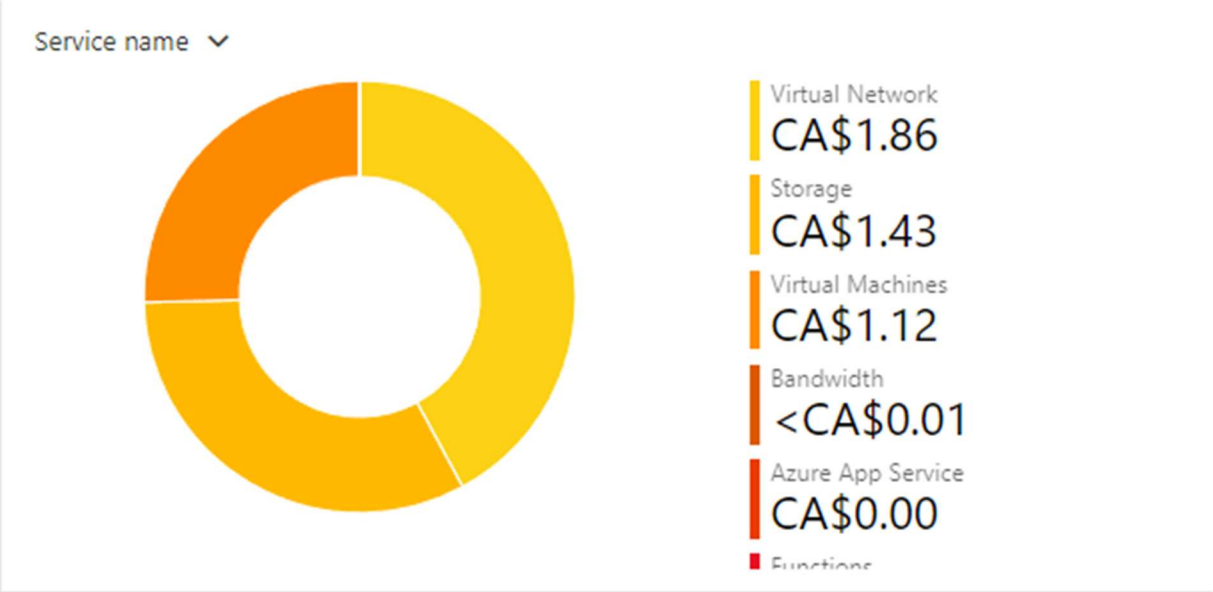
  - Lors de l'ajout des liens dans notre fichier html, les 2 compteurs essayés n'ont pas fonctionné. C'est pour cette raison que nous avons opté pour l'installation d'un IPS.

6. Un rapport de dépense Azure

- Estimé des dépenses du mois



- Répartition des coûts



7. Avis sur les technologies qui ont été utilisées dans ce projet.

- Azure :
  - La création du compte et de la machine fut aisée. Bien sûr, nos besoins étant minimes, nous n'avons pas exploré toutes les possibilités de configuration, nous contentant de la proposition de base. À l'utilisation, la plateforme semble être performante et les fonctionnalités offertes abondantes. Nous n'avons pas eu de soucis particuliers avec la plateforme durant le projet.

- Apache :
  - Le serveur Apache est un choix assez intéressant quand on regarde pour créer un site web. Celui-ci s'installe sur presque tous les systèmes d'exploitation et est bien documenté. Il faut cependant avoir une connaissance des commandes lorsque celui-ci s'utilise sans une interface graphique. Dans notre cas, l'installation sur Debian en ligne de code a dû être refait à quelques reprises lorsque nous avoir ''brisé'' notre site web. Il

a été simple de repartir à un point fonctionnel pour continuer. Nous nous sommes aussi rendu compte que le serveur Nginx pouvait interférer avec celui d'Apache. Nous avons donc désinstallé Nginx.

- Certbot :
    - En ce qui concerne Certbot, celui-ci effectue le travail de création de certificat sans avoir besoin de faire beaucoup de manipulation. Une fois le site web en place, l'installation et la certification se font en 2 lignes de code. Bien que le logiciel soit facile d'utilisation, il est somme toute assez peu transparent. En effet, la certification en entier se fait sans même nous donner d'information sur ce qui s'est passé. Pour nos besoins, celui-ci fut suffisant.

- Crowdsec :
    - Le choix d'utiliser Crowdsec est apparu lorsque nous avons rencontré des difficultés avec l'implantation d'un compteur de visite sur notre page, comme mentionné plus haut. Nous avons ensuite tenté l'installation de Fail2ban, mais celui-ci rencontrait aussi des problèmes. Nous avons cherché une alternative à Fail2ban et Crowdsec est apparu comme un choix intéressant. L'installation fut très facile et l'utilisation aussi. Après quelques temps de fonctionnement, il était déjà possible d'observer des alertes et décisions prisent par l'IPS en utilisant des commandes simples.
- Compteurs de visites :
    - Comme mentionné plus haut, notre tentative d'ajouter un compteur de visite à notre dit web fut infructueuse. Nous n'avons aucune idée de la raison du non-fonctionnement lorsqu'implanté sur notre serveur. Nous avons testé les commandes en local à l'aide de Visual Studio Code avec succès. Après une heure de recherche, nous avons décidé de faire autre chose. Nos recherches nous ont tout de même permis de trouver la cause probable de problème soit que notre configuration actuelle d' Apache pourrait bloquer les ressources externes (mod_proxy ou mod_headers de .htaccess).