

Table des matières

Détails de la machine virtuelle.....	2
Récupération de paramètres importants durant la phase test.....	2
Paramètres de l'instance Oracle ➔ liste de sécurité réseau (ports entrants autorisés).....	2
Paramètres Hestia.....	2
Pare-feu du panneau de configuration	2
Configurations globales.....	3
Paramètres des sites Web.....	6
Serveur mail Roundcube	8
Paramètres nom de domaine liam-le-may.fr (OVH).....	10
Informations utiles avant nouvelle installation.....	10
Installation de Hestia (https://gabizz.github.io/hestiacp-scriptline-generator/).....	10
Informations Apache.....	11
Liste de sécurité réseau Oracle Cloud.....	11
Paramètres SMTP pour le serveur mail.....	11
Restauration du portfolio Wordpress	11
Remarques importantes.....	12
Oracle Cloud Free Tier (https://www.oracle.com/fr/cloud/free/).....	12
SSH sur port 22.....	12
Utilisateurs Ubuntu	12
Remarques après-installation.....	12
Wordpress.....	12
OVH.....	12
Hestia.....	12
Webmail Roundcube.....	13

Détails de la machine virtuelle

Hébergeur	Oracle Cloud (Free tier)
CPU	ARM – 24 cœurs (VM.Standard.A1.Flex)
HDD	100 Go
RAM	24 Go
Bande passante	4 Gbit/s
Système d'exploitation	Ubuntu Server 20.04 LTS

Récupération de paramètres importants durant la phase test

Paramètres de l'instance Oracle → liste de sécurité réseau (ports entrants autorisés)

Règles entrantes (13)

Règles sortantes (1)

Ajouter des règles entrantes

Modifier

Enlever

<input type="checkbox"/>	Sans conservation de statut	Source	Protocole IP	Plage de ports source	Plage de ports de destination	Type et code	Autorise	Description
<input type="checkbox"/>	Non	0.0.0.0/0	TCP	Tout	22		Traffic TCP pour les ports : 22 SSH Remote Login Protocol	⋮
<input type="checkbox"/>	Non	0.0.0.0/0	ICMP			3, 4	Traffic ICMP pour : 3, 4 Destination inaccessible. La fragmentation est requise mais l'option Ne pas fragm enter a été définie	⋮
<input type="checkbox"/>	Non	10.0.0.0/16	ICMP			3	Traffic ICMP pour : 3 Destination in accessible	⋮
<input type="checkbox"/>	Non	0.0.0.0/0	TCP	Tout	8088		Traffic TCP pour les ports : 8088	⋮
<input type="checkbox"/>	Non	0.0.0.0/0	TCP	Tout	80		Traffic TCP pour les ports : 80	⋮
<input type="checkbox"/>	Non	0.0.0.0/0	TCP	Tout	443		Traffic TCP pour les ports : 443 HT TPS	⋮
<input type="checkbox"/>	Non	0.0.0.0/0	TCP	Tout	143		Traffic TCP pour les ports : 143 Int erm Mail Access Protocol (IMAP)	⋮
<input type="checkbox"/>	Non	0.0.0.0/0	TCP	Tout	993		Traffic TCP pour les ports : 993	⋮
<input type="checkbox"/>	Non	0.0.0.0/0	TCP	Tout	110		Traffic TCP pour les ports : 110 PO P3	⋮
<input type="checkbox"/>	Non	0.0.0.0/0	TCP	Tout	995		Traffic TCP pour les ports : 995	⋮
<input type="checkbox"/>	Non	0.0.0.0/0	TCP	Tout	25		Traffic TCP pour les ports : 25 Sim ple Mail Transfer Protocol (SMTP)	⋮
<input type="checkbox"/>	Non	0.0.0.0/0	TCP	Tout	465		Traffic TCP pour les ports : 465	⋮
<input type="checkbox"/>	Non	0.0.0.0/0	TCP	Tout	587		Traffic TCP pour les ports : 587	⋮

0 sélectionné(s)


Affichage de 13 éléments < 1 sur 1 >


Paramètres Hestia


Pare-feu du panneau de configuration


	Action	Commentaire	Protocole	Port	Adresse IP
<input type="checkbox"/>	✓ Permettre	PING	ICMP	0	0.0.0.0/0
<input type="checkbox"/>	✓ Permettre	HESTIA	TCP	8088	0.0.0.0/0
<input type="checkbox"/>	✓ Permettre	IMAP	TCP	143,993	0.0.0.0/0
<input type="checkbox"/>	✓ Permettre	POP3	TCP	110,995	0.0.0.0/0
<input type="checkbox"/>	✓ Permettre	SMTP	TCP	25,465,587	0.0.0.0/0
<input type="checkbox"/>	✓ Permettre	DNS	TCP	53	0.0.0.0/0
<input type="checkbox"/>	✓ Permettre	DNS	UDP	53	0.0.0.0/0
<input type="checkbox"/>	✓ Permettre	FTP	TCP	21,12000-12100	0.0.0.0/0
<input type="checkbox"/>	✓ Permettre	WEB	TCP	80,443	0.0.0.0/0
<input type="checkbox"/>	✓ Permettre	SSH	TCP	22	0.0.0.0/0

Configurations globales


 **Serveur Web**

Serveur proxy: nginx 

Serveur Web: apache2 

Serveur backend: php-fpm 

Versions PHP activées

 L'enregistrement des modifications peut prendre quelques minutes. Veuillez attendre la fin du processus et ne pas actualiser la page.

☐ php-5.6

☐ php-7.0



☐ php-7.1


☐ php-7.2

☐ php-7.3

☐ php-7.4

☒ php-8.0








☐ php-8.1


System PHP version


php-8.0



 **Serveur de courrier**

Serveur de courrier: exim4 

Antivirus: clamav-daemon 

AntiSpam: spamassassin 


Alias de messagerie Web (*webmail.example.com*)

webmail

☐ Relais SMTP global



Bases de Données ▾

MySQL Support 

Oui ▾

phpMyAdmin Alias

Ouverture de session unique pour phpMyAdmin *(More info)*

Désactivé ▾

Hôte #1

localhost

Mot de Passe

Nombre maximum de bases de données

500

Current Number Of Databases

1



Système



API

Activer l'accès à l'API

Oui

Adresses IP autorisées pour l'API

1 IP address per line

Se connecter

Style de l'écran de connexion

Défaut

Permettre aux utilisateurs de réinitialiser leurs mots de passe

Oui

Délai d'inactivité de la session (Minutes)

30

Prevent CSRF

Activé

Paramètres des sites Web

liam-le-may.fr

Domaine

liam-le-may.fr

Alias

www.liam-le-may.fr



Lets Encrypt obtiendra un nouveau certificat SSL si les alias de domaine web sont modifiés.

IP Address

144.24.193.79

Statistiques Web

none

☐ Activer la redirection de domaine

☒ Activer SSL pour ce domaine

☒ Utilisez Lets Encrypt pour obtenir un certificat SSL

☒ Activer la redirection HTTP vers HTTPS automatique

☒ Activer la sécurité de transport HTTP stricte (HSTS) ?

SUBJECT:	liam-le-may.fr
ALIASES:	liam-le-may.fr,www.liam-le-may.fr
NOT_BEFORE:	Jun 2 11:17:12 2022 GMT
NOT_AFTER:	Aug 31 11:17:11 2022 GMT
SIGNATURE:	sha256WithRSAEncryption
PUB_KEY:	4096 bit
ISSUER:	C = US, O = Let's Encrypt, CN = R3

[Show Certificate](#)

tpweb.liam-le-may.fr

Alias



Lets Encrypt obtiendra un nouveau certificat SSL si les alias de domaine web sont modifiés.

IP Address

144.24.193.79

Statistiques Web

none

☐ Activer la redirection de domaine

☒ Activer SSL pour ce domaine

- ☒ Utilisez Lets Encrypt pour obtenir un certificat SSL
- ☒ Activer la redirection HTTP vers HTTPS automatique
- ☒ Activer la sécurité de transport HTTP stricte (HSTS) ?

SUBJECT: tpweb.liam-le-may.fr
ALIASES: tpweb.liam-le-may.fr
NOT_BEFORE: Jun 2 12:47:07 2022 GMT
NOT_AFTER: Aug 31 12:47:06 2022 GMT
SIGNATURE: sha256WithRSAEncryption
PUB_KEY: 4096 bit
ISSUER: C = US, O = Let's Encrypt, CN = R3

[Show Certificate](#)

⇒ Possibilité de déplacer les fichiers du site Web depuis le gestionnaire de fichiers Hestia ou depuis `/home/<utilisateur_hestia>/web/.../public_html.`

Serveur mail Roundcube

Client Webmail

Roundcube

Pour liam-le-may.fr

Email de Récupération

☒ Support de l'AntiSpam

☒ Support de l'AntiVirus

☒ Activer DKIM

☒ Activer SSL pour ce domaine

☒ Utilisez Lets Encrypt pour obtenir un certificat SSL

!

webmail.liam-le-may.fr To enable Let's Encrypt SSL, ensure that DNS records exist for mail.liam-le-may.fr and webmail.liam-le-may.fr!

SUBJECT:

mail.liam-le-may.fr

Alias:

mail.liam-le-may.fr,webmail.liam-le-may.fr

NOT_BEFORE:

Jun 2 12:15:14 2022 GMT

NOT_AFTER:

Aug 31 12:15:13 2022 GMT

SIGNATURE:

sha256WithRSAEncryption

PUB_KEY:

4096 bit

ISSUER:

C = US, O = Let's Encrypt, CN = R3

☒ Relais de SMTP

Hôte

smtp-relay.sendinblue.com

Port

587

Nom d'utilisateur

Base de Données

97673

Nom d'Utilisateur (longueur maximale de 32 caractères, préfixe compris)

97673

Mot de Passe

Votre mot de passe doit avoir au moins:

- 8 caractères de long
- 1 majuscule et 1 caractère minuscule
- 1 numéro

**Mode automatique
laissé durant la
création de la BDD**

Type

mysql

Hôte

localhost

Charset

UTF8

Paramètres nom de domaine liam-le-may.fr (OVH)

<input type="checkbox"/> Domaine	TTL	Type	Cible	
<input type="checkbox"/> liam-le-may.fr	0	MX	10 liam-le-may.fr.	...
<input type="checkbox"/> liam-le-may.fr	0	A	144.24.193.79	...
<input type="checkbox"/> mail.liam-le-may.fr	0	A	144.24.193.79	...
<input type="checkbox"/> tpweb.liam-le-may.fr	0	A	144.24.193.79	...
<input type="checkbox"/> webmail.liam-le-may.fr	0	A	144.24.193.79	...
<input type="checkbox"/> www.liam-le-may.fr	0	A	144.24.193.79	...
<input type="checkbox"/> liam-le-may.fr	0	CAA	0 issue "letsencrypt.org"	...
<input type="checkbox"/> liam-le-may.fr	0	TXT	"Sendinblue-code:ee12bf14fd252a9700da2a4624252504"	...
<input type="checkbox"/> liam-le-may.fr	0	TXT	"v=spf1 include:spf.sendinblue.com mx ~all"	...
<input type="checkbox"/> _dmarc.liam-le-may.fr	0	TXT	"v=DMARC1; p=none; sp=none; rua=mailto:dmarc@mailinblue.com!10m; ruf=mailto:dmarc@mailinblue.com!10m; rf=afrf; pct=100; ri=86400"	...
<input type="checkbox"/> mail._domainkey.liam-le-may.fr	0	TXT	"k=rsa;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDeMVLzrCa3T14JsNY0lRv5/2V1/v2itviLQBwXsa7shBD6TrBkswsFUToPyMRWC9tbR/5ey0nRBH0ZVxp+lsMTxid2Y2z+FAPQ6ra2VsXfbJP3HE6wAO0YTVEJt1TmeczhEd2Jiz/fcablISgXEdSpTYJhb0ct0VJRxcg4c8c7wIDAQAB"	...

Paramètres à ne pas changer : Relai SMTP & authentification certificat SSL

Changer l'adresse IP pour chaque nouvelle instance

Informations générales Zone DNS Serveurs DNS **Redirection** DynHost GLUE Tâches récentes

Gérer ici les redirections de vos domaines et sous domaine vers d'autres adresses web ou vers des serveurs.

Domaine	Type	Cible	
<input type="checkbox"/> liam-le-may.fr	vers un serveur (ipv4 - A)	144.24.193.79	...
<input type="checkbox"/> mail.liam-le-may.fr	vers un serveur (ipv4 - A)	144.24.193.79	...
<input type="checkbox"/> tpweb.liam-le-may.fr	vers un serveur (ipv4 - A)	144.24.193.79	...
<input type="checkbox"/> webmail.liam-le-may.fr	vers un serveur (ipv4 - A)	144.24.193.79	...
<input type="checkbox"/> www.liam-le-may.fr	vers un serveur (ipv4 - A)	144.24.193.79	...

Adresses IP à changer

Tous Filtre sous domaine...

« < 1 > » 20 Page 1 / 1 OK

Informations utiles avant nouvelle installation

Installation de Hestia (<https://gabizz.github.io/hestiacp-scriptline-generator/>)

⇒ Se connecter sous root

wget <https://raw.githubusercontent.com/hestiacp/hestiacp/release/install/hst-install.sh>

```
sudo bash hst-install.sh --apache yes --phpfpm yes --multiphp no --vsftpd no --proftpd no --named yes --mysql yes --postgresql no --exim yes --dovecot yes --sieve no --clamav yes --spamassassin yes --iptables yes --fail2ban yes --quota no --api yes --interactive no --with-debs no --port 8088 --hostname hcp.liam-le-may.fr --email *****@*****.* --password <mot de passe> --lang fr --force
```

⇒ **Mot de passe dans la commande d'installation : pas de caractères spéciaux !**

Informations Apache

Les modules ssl et rewrite sont activés par défaut avec Hestia → **activer manuellement headers (a2enmod headers)**

- **Installer le paquet libapache2-mod-security2**
- Renommer *etc/modsecurity/modsecurity.conf-recommended* en *etc/modsecurity/modsecurity.conf*
- Aller dans */etc/modsecurity/modsecurity.conf* :
 - o Noter « SecServerSignature oui »
- Aller dans */etc/apache2/conf-available/security.conf* :
 - o Passer le ServerTokens en Full

⇒ **Ajouter également les directives de sécurité dans */etc/apache2/apache2.conf*.**

Liste de sécurité réseau Oracle Cloud

Ports à autoriser en entrant depuis l'adresse 0.0.0.0/0 : **8088,80,443,143,993,110,995,25,465,587**

Depuis Oracle : Fonctions de réseau → Réseaux cloud virtuels → ... → Détails du sous réseau → Liste de sécurité par défaut

Règle entrante 1

Autorise le trafic TCP 8088,80,443,143,993,110,995,25,465,587

☐ Sans conservation de statut ⓘ

Type de source CIDR source Protocole IP ⓘ

CIDR 0.0.0.0/0 TCP

Adresses IP spécifiées : 0.0.0.0-255.255.255.255 (adresses IP 4 294 967 296)

Plage de ports source Facultatif ⓘ Plage de ports de destination Facultatif ⓘ

Tout 8088,80,443,143,993,110,995,25,465,587

Exemples : 80, 20-22 Exemples : 80, 20-22

Description Facultatif ⓘ

255 caractères au maximum

Paramètres SMTP pour le serveur mail

Clé SMTP : xsmtpsib-*****

Hôte SMTP : smtp-relay.sendinblue.com

Port : 587

Nom d'utilisateur : *****@*****.***

Restauration du portfolio Wordpress

Installer Wordpress normalement, installer le plugin Updraft Backup and Restore et restaurer le site à partir de la dernière sauvegarde enregistrée sur Google Drive.

Par la suite, restaurer les dernières lignes du fichier .htaccess du portfolio

Remarques importantes

Oracle Cloud Free Tier (<https://www.oracle.com/fr/cloud/free/>)

Pour la formule toujours gratuite → 4 cœurs Ampere A1 basés sur Arm et 24 Go de mémoire utilisables comme une seule VM ou jusqu'à 4 VM + 2 volumes de blocs de stockage, 200 Go au total.

SSH sur port 22

Utiliser les certificats générés par Oracle lors de la création de l'instance et les convertir en format PuTTY → **NE PAS MODIFIER LES PARAMETRES SSH SUR UBUNTU → DETRUIT L'ACCES SSH DE LA MACHINE**

Utilisateurs Ubuntu

Garder l'utilisateur Ubuntu de base cependant, **CHANGER LE MOT DE PASSE DU COMPTE AVEC PASSWD UBUNTU** → permet de pouvoir retrouver accès à la machine en cas de problème avec SSH.

Remarques après-installation

Wordpress

Le fichier .htaccess ne s'était pas restauré après la restauration de Updraft backup → restauration manuelle nécessaire sinon liens personnalisés non fonctionnels.

Le plugin Updraft sauvegardes et backup n'était plus fonctionnel sur la partie sauvegarde vers le cloud : impossible de sauvegarder vers mon Google Drive alors que le plugin avait été réinitialisé et la base de données nettoyée → passage vers le plugin WPvivid backup, depuis les sauvegardes sont fonctionnelles.

Lors de la création du site Wordpress depuis Hestia → **Indiquer un mot de passe personnalisé pour la base de données car il n'est pas indiqué après** (aller vérifier le fichier wp_config.php si jamais le mot de passe n'est pas connu/oublié).

OVH

Mise à jour des entrées A sur la zone DNS de liam-le-may.fr → **Supprimer les entrées au lieu de les mettre à jour** : la mise à jour des entrées ne met pas à jour la zone DNS instantanément alors que la suppression/création.

Hestia

Pour donner les accès SSH aux comptes créés, aller dans les paramètres de l'utilisateur concerné → paramètres avancé → accès « bash » à la connection SSH :

USER WEB DNS MAIL CRON BACKUP

Retour Gérer les clés SSH Journaux connexion en tant que Supprimer Sauvegarde

- 8 caractères de long
- 1 majuscule et 1 caractère minuscule
- 1 numéro

☐ Ne pas autoriser l'utilisateur à se connecter au Panneau de contrôle
☐ Activer l'authentification à deux facteurs
☐ Utiliser la liste des adresses IP autorisées pour les tentatives de connexion

Langue
French (Français)

Rôle
Utilisateur

Paquet
default

Options avancées 1

Accès SSH
nologin 2

Version de la ligne de commande PHP
8.0

Nom de Serveurs par Défaut
ns1.liam-le-may.fr
ns2.liam-le-may.fr
Ajouter un autre Serveur de Noms

Webmail Roundcube

Pour ajouter le(s) compte(s) créé(s), par exemple dans Thunderbird, **rentrer les informations de connexion manuellement au lieu de le faire en automatique** → réglages de sécurité incorrects en automatique :

UTILISER LE NOM D'HÔTE DU DOMAINE

Nom d'utilisateur:	contact@liam-le-may.fr
Mot de Passe:	
Nom d'hôte IMAP:	mailliam-le-may.fr
Port IMAP:	143
Sécurité IMAP:	STARTTLS
Méthode d'authentification IMAP:	Mot de passe normal
Nom d'hôte SMTP:	mailliam-le-may.fr
Port SMTP:	587
Sécurité SMTP:	STARTTLS
Méthode d'authentification SMTP:	Mot de passe normal
Alias de messagerie Web:	http://webmail.liam-le-may.fr

Paramètres du serveur

Type de serveur : Serveur de courrier IMAP

Nom du serveur :	<input type="text" value="mail.liam-le-may.fr"/>	Port :	<input type="text" value="143"/>	<input type="button" value="↑"/> <input type="button" value="↓"/>	Défaut : 143
Nom d'utilisateur :	<input type="text" value="contact@liam-le-may.fr"/>				

Paramètres de sécurité

Sécurité de la connexion :	<input type="text" value="STARTTLS"/>
Méthode d'authentification :	<input type="text" value="Mot de passe normal"/>

Détails du serveur sélectionné :

Description :	<non spécifié>
Nom du serveur :	mail.liam-le-may.fr
Port :	587
Nom d'utilisateur :	contact@liam-le-may.fr
Méthode d'authentification :	Mot de passe normal
Sécurité de la connexion :	STARTTLS