Connection Management Center 1.3

Guide d'installation

Dernière mise à jour : 28 mars 2025
Référence du document : 20250328_IG_CMC_1.3_FR_1.0

www.thegreenbow.com

TheGreenBow est un nom commercial déposé.

Microsoft, Windows 10 et Windows 11 sont soit des marques déposées, soit des marques commerciales de Microsoft Corp. aux États-Unis et/ou dans d'autres pays.

Linux® est une marque déposée par Linus Torvalds aux États-Unis et dans d'autres pays.

Ubuntu et le logo Ubuntu logo sont soit des marques déposées, soit des marques commerciales de Canonical Group Ltd. au Royaume-Uni, d'autres pays, ou les deux.

Red Hat, Red Hat Enterprise Linux, le logo Red Hat, le logo Shadowman, CentOS, JBoss, OpenShift, Fedora, le logo Infinity, et RHCE sont des marques déposées de Red Hat, Inc. aux États-Unis et dans d'autres pays.

Debian est une marque déposée de Software in the Public Interest, Inc. aux États-Unis, gérée par le projet Debian.

Apple, le logo Apple, iPhone, iOS, Mac et macOS sont des marques d'Apple Inc., déposées aux États-Unis et dans d'autres pays et régions.

Android, Google Chrome, Google Play et le logo Google Play sont des marques commerciales de Google, LLC.

HashiCorp, le logo HashiCorp, Consul, Nomad, Terraform et Vault sont des marques de HashiCorp Inc. déposées aux États-Unis et dans d'autres pays.

D'autres marques de commerce appartenant à des tiers et mentionnées dans ce document demeurent la propriété intellectuelle de ces tiers.

Toutes les informations fournies sont sujettes à modification à tout moment et sans préavis.

Malgré tous les soins apportés à la réalisation de ce document et à sa mise à jour régulière, des erreurs peuvent s'être glissées dans les informations présentées. Si vous en constatez n'hésitez pas à nous le faire savoir en nous contactant, nous procéderons aux rectifications correspondantes.

Table des matières

Tableau des révisions

Version	Date	Sections/pages affectées	Description de la modification	Auteur
1.0	2025-03-28	Toutes	Version initiale	ALE, FMA, VMA, BB

1 Présentation

1.1 Introduction

Merci d'avoir choisi le logiciel Connection Management Center (CMC).

Ce document décrit succinctement le fonctionnement du CMC et comment l'installer. L'installation sera effectuée par les équipes du client avec l'assistance de spécialistes TheGreenBow.

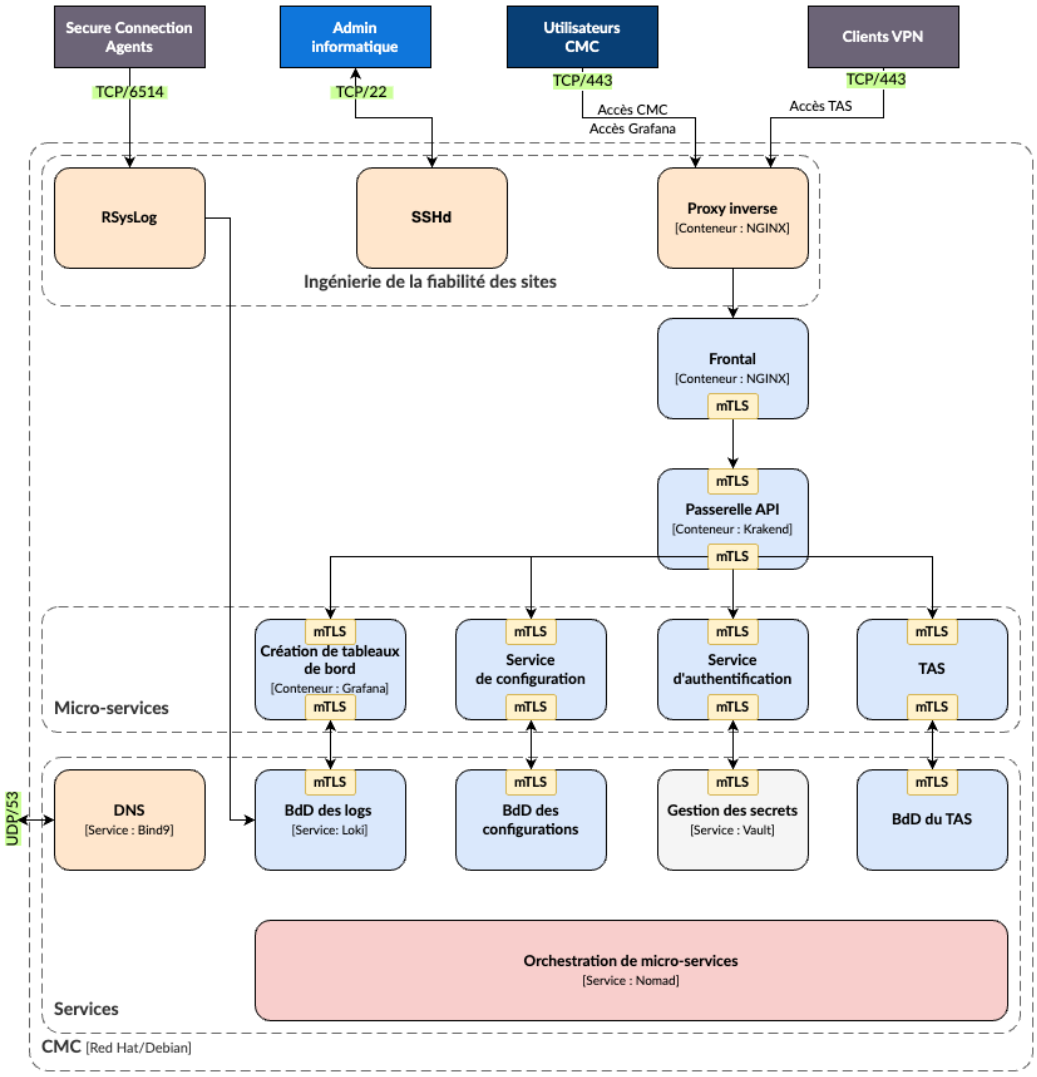
1.2 Fonctionnement du CMC

Le CMC est un logiciel serveur qui réalise les quatre principales fonctionnalités suivantes :

- Centralisation et affichage des logs provenant de l'ensemble du parc de Clients VPN TheGreenBow
- Gestion de l'activation des Clients VPN TheGreenBow par l'intégration du serveur d'activation (TAS)
- Gestion centralisée des configurations VPN à utiliser avec les différents Clients VPN du parc
- Gestion des utilisateurs du CMC

1.2.1 Architecture du produit

Le schéma suivant présente une architecture simplifiée du CMC :



Comme on peut le voir en haut du schéma, le CMC interagit à la fois avec des logiciels (Secure Connection Agents et Clients VPN) et des humains (administrateur informatique, utilisateurs du CMC).

Le CMC est constitué de plusieurs couches, dont :

- une couche de fiabilité (*Site Reliability Engineering* ou SRE en anglais),
- un frontal,
- une couche de micro-services,
- une couche de services avec un orchestrateur de micro-services.

1.2.2 Flux réseau

Dans la figure ci-dessus, les flux de données avec l'extérieur du CMC sont indiqués en vert avec le protocole et le port utilisés. En voici un récapitulatif :

Source	Destination	IP source	IP dest.	Port src.	Port dest.	Description
Pilote	CMC	@Pilote	@CMC	Any	TCP/22	SSH
Pilote	CMC	@Pilote	@CMC	Any	TCP/53 UDP/53	DNS
Pilote	CMC	@Pilote	@CMC	Any	TCP/443	HTTPS
Pilote	CMC	@Pilote	@CMC	Any	TCP/80	HTTP
Pilote	CMC	@Pilote	@CMC	Any	TCP/8200	
CMC	CMC	127.0.0.1	127.0.0.1	Any	Any	Aucun filtrage

Les flux de données au sein du CMC sont authentifiés par TLS mutuel (mTLS).

2 Configuration requise

Avant de procéder à l'installation du CMC, il convient de préparer l'environnement conformément aux indications ci-dessous.

2.1 Référence

Pour la préparation de l'environnement, suivre les *Recommandations relatives à l'administration sécurisée des systèmes d'information* de l'ANSSI : https://www.ssi.gouv.fr/uploads/2018/04/anssi-guide-admin_securisee_si_v3-0.pdf.

L'hypothèse retenue est la suivante :

- l'administrateur du CMC est un opérateur du client en intervention sur site ;
- le réseau cible est cloisonné.

Ce cas étant le plus contraignant, nous en faisons le cas général :

- la machine pilote est dédiée et seul l'outillage utile est installé à partir d'une image Docker pilotée par un script ;
- le déploiement est opéré via SSH et HTTPS ;
- un dépôt de paquets système et d'images de conteneurs est exploité sur la machine pilote durant l'exécution de l'installation et de la mise à jour.

2.2 Environnement technique

L'installation du CMC requiert deux machines :

- une machine CMC sur laquelle sera déployé le logiciel serveur CMC ;
- une machine pilote pour l'installation et l'administration de la machine CMC (fournie par le client).

Les caractéristiques requises de chacune de ces machines ainsi que d'autres prérequis sont listés dans les sections suivantes.

Les deux machines doivent se trouver dans le même réseau et utiliser le même fuseau horaire.

2.2.1 Machine CMC

La machine CMC (serveur de production) sur laquelle sera déployé le logiciel serveur CMC doit être fournie par le client final. Pour le bon déroulement de l'installation du CMC depuis la machine pilote, il est essentiel que la distribution installée sur celle-ci n'ait subi aucune modification ni

configuration personnalisée destinée à en renforcer la sécurité. Les principes de sécurité, de minimisation et de durcissement sont implémentés dans le produit et TheGreenBow les met en œuvre durant le processus d'installation.

La machine CMC doit en outre présenter les caractéristiques suivantes :

- Debian 12 « Bookworm » ou Red Hat 9.4/9.5, nouvelle installation configurée comme décrit ci-après
- 16 Go RAM
- 4 processeurs, architecture x86-64
- 2 volumes de stockage LVM dont le partitionnement est détaillé ci-après :
  - un volume de 60 Go pour les points de montage `/`, `/boot`, `/home`, `/opt`, `/tmp` et `swap`
  - un volume de 160 Go pour les points de montage `/var` et `/var/lib/loki`

Le partitionnement des volumes de stockage LVM doit être réalisé comme suit :

Volume 1 (60 GB)

Point de montage	Type de système de fichiers	Groupe de volume	Volume logique	Taille
`swap`	swap	N/A	N/A	6 Go
`/boot`		N/A	N/A	1 Go
`/`	ext4	`vg_root`	`lv_root`	20 Go
`/home`	ext4	`vg_root`	`lv_home`	10 Go
`/opt`	ext4	`vg_root`	`lv_opt`	20 Go
`/tmp`	ext4	`vg_root`	`lv_tmp`	1 Go

Volume 2 (160 GB)

Point de montage	Type de système de fichiers	Groupe de volume	Volume logique	Taille
`/var`	ext4	`vg_var`	`lv_var`	30 Go
`/var/lib/loki`	ext4	`vg_var`	`lv_var`	120 Go

Ces partitions doivent être extensibles.

- IP statique dédiée à la machine CMC

- Route par défaut dans la table de routage (par défaut ou 0.0.0.0), exemple :

```
ip r
default via 192.168.252.2 dev ens33 proto static
192.168.252.0/24 dev ens33 proto kernel scope link src
192.168.252.115
```

- 1 DNS local unique en 127.0.0.1 (`/etc/resolv.conf`), exemple :

```
more /etc/resolv.conf
domain localdomain
search localdomain
nameserver 127.0.0.1
```

⚠ Assurez-vous de désactiver les daemons ou services qui sont susceptibles de prendre le contrôle sur le fichier `/etc/resolv.conf` (p. ex. `systemd-resolved`, NetworkManager ou autre).

Par exemple, pour NetworkManager, procédez comme suit :

a) Éditez le fichier de configuration de NetworkManager :

```
sudo nano /etc/NetworkManager/NetworkManager.conf
```

b) Ajoutez la directive suivante dans le fichier de configuration :

```
[main]
dns=none
```

c) Redémarrez le service :

```
systemctl restart NetworkManager
```

- Serveur SSH avec `PermitRootLogin` à `yes` de manière temporaire (pour lancer le déploiement). Un script révoque ce droit à l'issue du déploiement. Vérifier la bonne mise en place de l'option :

```
cat /etc/ssh/sshd_config | grep PermitRootLogin
```

- Dépôts APT à jour après installation de l'OS, exemple pour Debian :

```
apt update
apt upgrade
```

Exemple pour Red Hat :

```
dnf upgrade
```

- Image instantanée (ou *snapshot*) de l'état de la machine avant déploiement, une fois tous les prérequis ci-dessus réalisés
- Pas de filtrage `IPtable` sur `localhost`

2.2.2 Machine pilote

La machine pilote utilisée pour l'installation et l'administration de la machine CMC doit être fournie par le client et présenter les caractéristiques suivantes :

- Distribution Linux Debian 12 ou Red Hat 9.4/9.5 pour CPU x86-64 (de préférence une machine virtuelle de production)
- Support de stockage avec 50 Go d'espace libre ; s'assurer d'avoir 20 Go d'espace disponible pour le dossier `/var` et 20 Go d'espace disponible pour le dossier `/home`
- Logiciel `netcat` à jour installé en tant que `root` avec APT sur Debian :

```
apt update
apt upgrade -y
apt install netcat-traditional -y
```

ou avec DNF sur Red Hat :

```
dnf install ncat
```

- Logiciel Docker à jour installé depuis le dépôt Docker :

```
docker-ce-cli containerd.io docker-buildx-plugin docker-
compose-plugin
```

- Logiciel SELinux installé et configuré en mode permissif. Pour cela, ouvrez le fichier de configuration en édition :

```
nano /etc/selinux/config
```

Puis, configurez l'option `SELINUX=permissive`.

- Navigateur récent
- Archive d'installation du CMC récupérée
- Capacité de résolution du sous-domaine délégué au CMC
- Fichier de configuration `config.yml` (cf. 3.2.8 Contenu du fichier de configuration)
- Script des prérequis exécuté sur la machine pilote et validation des prérequis avec l'équipe TheGreenBow
- Présence du fichier de sauvegarde du TAS (cf. 2.2.4 Préparation du TAS)
- Si l'option TAS est retenue, fichier de configuration `config.yml` avancé
- Synchronisation des dates entre les machines
- Ouverture des ports 443, 6514, 22, 53, 80, 8200 pour les flux réseau utilisés par le CMC

2.2.3 Certificats

Si le CMC doit s'intégrer à la PKI de l'entreprise ou de l'organisation, le client final doit fournir les éléments suivants :

- Chaîne de certificats CA
  - `ca.cert.pem` : certificats CA intermédiaire et racine en mesure de valider le certificat du CMC
- Certificat du CMC
  - `self.cert.pem` : certificat terminal[1] à clé publique du CMC
  - `self.cert.key` : clé privée du CMC
  - `self.fullchain.cert.pem` : chaîne de certification complète composée du certificat terminal à clé publique du CMC (sans la clé privée) et des certificats CA et intermédiaire le validant
- Certificat du SCA (agent sur le poste client)
  - `subclient.fullchain.cert.pem` : certificats CA intermédiaire et racine en mesure de valider un certificat présenté par un agent SCA

Les deux types de certificats suivants sont compatibles avec le CMC :

- **[recommandé]** Certificat SAN ou multi-domaine, qui couvre explicitement tous les sous-domaines gérés par le CMC :
  - Nom commun[2] (CN) : `<cmc.vmlab.lan>`

[1] Ou *leaf certificate* en anglais.
[2] Ou *Common Name* en anglais.

  - Autre nom de sujet[1] (SAN) :
    - `DNS:<www.cmc.vmlab.lan>`
    - `DNS:<tas.cmc.vmlab.lan>`
    - `DNS:<vault.cmc.vmlab.lan>`
    - `DNS:<consul.cmc.vmlab.lan>`
    - `DNS:<nomad.cmc.vmlab.lan>`
    - `DNS:<grafana.cmc.vmlab.lan>`
    - `DNS:<loki.cmc.vmlab.lan>`
    - `DNS:<promtail.cmc.vmlab.lan>`
    - `DNS:<prometheus.cmc.vmlab.lan>`
    - `DNS:<cmc-mono.cmc.vmlab.lan>`
- Certificat générique[2], qui couvre le domaine délégué au CMC et tous ses sous-domaines :
  - Nom commun (CN) : `*.<cmc.vmlab.lan>`
  - Autre nom de sujet (SAN) : `DNS:<*.cmc.vmlab.lan>`, `DNS:<cmc.vmlab.lan>`

Le certificat du CMC doit avoir les propriétés supplémentaires suivantes :

- Extended key usages :

Usage	OID
Server authentication	1.3.6.1.5.5.7.3.1
Client authentication	1.3.6.1.5.5.7.3.2

2.2.4 Préparation du TAS

Le serveur d'activation TheGreenBow Activation Server (TAS) fait désormais partie intégrante du CMC.

Lors du déploiement du CMC, les deux scénarios suivants peuvent se présenter pour le service TAS :

- **Migration du TAS**, si le client est déjà utilisateur du TAS ;
- **Nouvel utilisateur TAS**, si le client souhaite mettre en place ce service.

[1] Ou *Subject Alternative Name* en anglais.
[2] Ou *wildcard certificate* en anglais.

Procédure commune

Quel que soit le scénario, la procédure est identique sauf pour l'étape 2. Pour préparer le TAS, procédez comme suit :

1. Récupérez les informations suivantes en passant par le support client le cas échéant :
   - DB name, se trouve dans le fichier `settings.php` sur le serveur TAS
   - DB private, se trouve dans le fichier `settings.php` sur le serveur TAS
   - OSA code, se trouve dans l'interface du TAS, menu **A propos** > **TAS Name** > **ID**

Scénario Migration du TAS

Dans ce cas, l'objectif est de migrer les données du client de son instance de TAS existante vers le service d'activation du CMC.

2. Exécutez les commandes suivantes pour vider la base de données du TAS (créer un *dump*) du client :

```
bash
mysqldump --datatabes <DB name> <DB private> \
--user=<xxxx> --password=<xxxxx> \
--add-drop-database > mariadb tas.sql
```

⚠ Les dump SQL doivent comporter les directives `DROP DATABASE IF EXISTS` avant chaque commande `CREATE DATABASE`.

Scénario Nouvel utilisateur TAS

Dans ce cas, l'objectif est de déployer le service TAS chez un nouvel utilisateur.

2. Le fichier `osace.sql` vous est fourni par l'équipe TheGreenBow.

Suite de la procédure commune

3. Copiez le fichier `osace.sql` dans le répertoire `config` de déploiement du CMC.

4. Préparez le fichier de déploiement du CMC `config.yml` pour y ajouter les informations relatives au profil client TAS.

Ces informations sont à insérer en complément des autres informations à renseigner dans le fichier de configuration (cf. 3.2.8 Contenu du fichier de configuration).

3 Mise en œuvre des prérequis avant l'installation

3.1 Machine CMC

3.1.1 IP statique

Une adresse IP statique doit être dédiée au CMC.

3.1.2 Route par défaut

Lancer la commande suivante :

```
ip r
```

La sortie doit indiquer une route par défaut et une seule comme suit :

```
$ ip r
default via 192.168.252.2 dev ens33 proto static
192.168.252.0/24 dev ens33 proto kernel scope link src
192.168.252.115
```

Si ce n'est pas le cas, utiliser le gestionnaire de réseau actif sur votre machine (`/etc/network`, `systemd-network`, `NetworkManager`...) pour ajouter une route par défaut.

3.1.3 Vérification du DNS

L'IP du DNS doit être local (127.0.0.1), car il fait autorité sur le sous domaine.

```
$ more /etc/resolv.conf
domain localdomain
search localdomain
nameserver 127.0.0.1
```

Le serveur de noms (ou *name server* en anglais) est `127.0.0.1`.

3.1.4 Serveur SSH

Le déploiement tel que présenté sur le schéma de principe de l'installation (cf. section 4.1 Principe de l'installation), est opéré depuis la machine pilote. La machine pilote utilise Ansible sur le protocole SSH afin de déployer le CMC sur la machine cible. À ce titre, la machine cible doit disposer d'un serveur SSH opérationnel et permettant l'accès SSH à l'utilisateur root via une clé SSH.

La directive suivante doit donc être présente dans le fichier `/etc/ssh/sshd_config` :

```
PermitRootLogin yes
```

Pour vérifier la bonne prise en compte de la configuration :

```
cat /etc/ssh/sshd_config | grep PermitRootLogin
```

L'accès SSH root est automatiquement supprimé après l'installation. Aucune intervention de l'utilisateur n'est nécessaire.

3.1.5 Dépôts logiciels à jour

Après installation de l'OS sur la machine cible, exécutez la commande suivante pour Debian :

```
apt update
apt upgrade
```

Et pour Red Hat:

```
dnf upgrade
```

3.1.6 Python3

Nous utilisons `python3-{dnf|apt}` pour interagir avec le gestionnaire de paquets via Python. Ce paquet offre une interface Python pour gérer les paquets, les dépôts et le cache. C'est pourquoi il convient de vérifier que Python3 est bien installé sur la machine.

Pour Debian, exécutez la commande suivante :

```
apt policy python3-apt
```

Vérifiez que la commande retourne les éléments suivants :

```
python3-apt
  Installé : 2.X.Y
  Candidat : 2.X.Y
```

Pour Red Hat, exécutez la commande suivante :

```
dnf info --installed python3-dnf
```

Vérifiez que la commande retourne les éléments suivants :

```
Paquets installés
Nom         : python3-dnf
Version     : 4.X.Y
```

3.2 Machine pilote

3.2.1 Vérification de la connectivité vers la machine CMC

Il est nécessaire de vérifier la connectivité de la machine pilote avec le CMC :

```
nc -zv [adresse_IP_du_CMC] 22
```

Réponse attendue :

```
Connection to [adresse_IP_du_CMC] 22 port [tcp/ssh]
succeeded!
```

3.2.2 Configuration DNS

Le serveur DNS configuré sur la machine doit permettre de résoudre les FQDN du CMC, p. ex. `www.<cmc.domaine.lan>`.

```
[adresse_IP_du_CMC] www.cmc.domaine.lan
nomad.cmc.domaine.lan vault.cmc.domaine.lan
grafana.cmc.domaine.lan consul.cmc.domaine.lan
```

Si le réseau ne dispose pas de serveur DNS, les adresses FQDN du CMC peuvent être inscrites dans le fichier `/etc/hosts`.

3.2.3 Vérification de la délégation DNS

Il convient de vérifier que la résolution DNS est valide :

```
more /etc/resolv.conf
nameserver [ip_dns]
```

Dans l'exemple ci-dessus, `ip_dns` correspond à l'adresse IP du serveur DNS qui délègue la zone au CMC.

3.2.4 Rendre disponible l'archive d'installation du CMC

Afin de préparer le déploiement, une archive contenant l'image de la version du CMC à déployer vous est fournie accompagnée de sa signature. L'archive est fractionnée en plusieurs fichiers se terminant par une extension `*.gzaa`, `*.gzab`, `*gzac`, etc.

Commencez par créer l'image du CMC en reconstituant l'archive à partir des fichiers fractionnés. Pour cela, exécutez la commande suivante dans le répertoire de téléchargement :

```
cat cmc-offline-[distribution]-1.3.b.tar.gza* > cmc-
offline-[distribution]-1.3.b.tar.gz
```

Remplacez `[distribution]` par la distribution concernée (`rhel` ou `debian`) et b par le numéro de *build*.

Cette archive contient tout le nécessaire au déploiement du CMC.

Exécutez la commande suivante pour confirmer que l'archive est valide pour le déploiement :

```
sha256sum cmc-offline-[distribution]-1.3.b.tar.gz |
sha256sum -c ./cmc-offline-[distribution]-1.3.b.sha256
```

Remplacez `[distribution]` par la distribution concernée (`debian` ou `rhel`) et b par le numéro de *build*.

⚠ Cette étape doit être réalisée avant le déploiement, mais pas nécessairement par le client final.

3.2.5 Préparation du déploiement

La structure de répertoires suivante doit être présente pour lancer le déploiement du CMC. Le nom du dossier `instance_cmc` est indifférent. Vous pouvez choisir le nom que vous voulez.

```
<instance_cmc>
\ <inventories>                    DOIT être vide pour nouveau déploiement
\ <config>
  | mariadb_tas.sql                (optionnel) Fichier de restauration TAS
  | config.yml                     Fichier config. déploiement
  \ <secrets>
    | ca.cert.pem                  Certificats CA sub & root CMC
    | default.key                   Clé privée SSH
    | default.key.pub               Clé publique SSH
    | self.cert.key                 Clé privée CMC
    | self.cert.pem                 Certificat à clé publique CMC
    | self.fullchain.cert.pem       Chaîne de cert complète CMC
    | subclient.fullchain.cert.pem  (optionnel) Certificats CA sub & root SCA
```

⚠ Pour éviter toute erreur lors de l'installation, il convient de s'assurer que le répertoire `inventories` est bien vide sur la machine pilote.

La configuration se trouve sous ce chemin :

```
$PWD/inventories/hs_$WORKSPACE/group_vars/hashistack/out
.stage0.cmc.yml
```

3.2.6 Créer le dossier de base

Lancez la commande suivante pour créer un dossier de base :

```
mkdir -p instance_cmc/{config/secrets,inventories}
```

3.2.7 Créer le fichier de configuration

Lancez la commande suivante pour créer le fichier de configuration :

```
nano instance_cmc/config/config.yml
```

Ne pas créer le fichier `config.yml` sous Windows, car les retours chariots (`\r\n`) sont différents de ceux de Debian et Red Hat (`\n`) et ne sont pas pris en charge.

3.2.8 Contenu du fichier de configuration

Le fichier de configuration `config.yml` contient les informations suivantes :

- `cmc_name` [obligatoire] : nom de l'instance du CMC
- `cmc_domain` [obligatoire] : nom du domaine hébergeant le CMC (dans l'exemple précédent, l'instance de CMC sera joignable à l'adresse `cmc.domaine.lan`)
- `cmc_user` [obligatoire] : root (utilisateur qui pilote)
- `cmc_type` [obligatoire] : mono (type d'instance du CMC)
- `cmc_ipv4` [obligatoire] : adresse IP statique du CMC
- `cmc_dns` [obligatoire] : adresse IP du serveur DNS gérant le domaine sur lequel le CMC est déployé

Plus cinq paramètres pour la restauration de la base de données du TAS, uniquement si la migration du TAS ou un nouvel utilisateur TAS est prévu (cf. 2.2.4 Préparation du TAS) :

- `tas_db_name` [facultatif] : nom de la base de données TAS
- `tas_db_private` [facultatif] : nom de la base de données privée du TAS
- `tas_osa_code` [facultatif] : code OSA du TAS
- `tas_db_sql_file` [facultatif] : chemin vers le fichier SQL de dump du TAS
- `tas_licence` [facultatif] : si ce paramètre n'est pas fourni, le service TAS ne peut pas être activé

Depuis la version 1.3 du CMC, il est désormais possible de personnaliser les ports d'écoute des services, notamment pour séparer les flux réseaux liés à l'activation des clients VPN de ceux liés à l'utilisation du CMC via l'interface web. Dans ce but, vous pouvez ajouter les paramètres suivants :

- `tas_activation_port` [facultatif] :port personnalisé à utiliser pour le service d'activation du CMC ; **par défaut : 443**
- `syslog_port` [facultatif] : port personnalisé à utiliser pour la remontée des logs chiffrés ; **par défaut : 6514**

Si vous ne voulez pas personnaliser ces ports et utiliser les ports par défaut, ne renseignez pas ces paramètres.

Il convient de préparer ce fichier comme suit (exemple) :

```
---
cmc_name: cmc
cmc_domain: domaine.lan
cmc_user: root
cmc_type: mono
cmc_ipv4: "192.168.1.87"
cmc_dns: ["192.168.1.253"]
tas_db_name: "customer_tas_db_name"
tas_db_private: "customer_tas_db_private"
tas_osa_code: customer_tas_osa_code
tas_db_sql_file: /opt/cmc/config/osace.sql
tas_licence: 123456-789012-345678-901234
tas_activation_port: 9443
syslog_port: 6443
```

3.2.9 Migration du TAS

Copiez le fichier de vidage (ou *dump file* en anglais) `osace.sql` dans le répertoire `instance_cmc/config` de déploiement du CMC.

3.2.10 Transfert de fichier via SSH

Une clé SSH de type ed25519 sans mot de passe doit être générée pour les transferts SSH.

Un accès `root` à la machine CMC doit être activé via la clé SSH ed25519. Cet accès est octroyé de manière temporaire le temps du déploiement. Il est automatiquement révoqué à l'issue du déploiement.

3.2.10.1 Générer la clé SSH

Lancez les commandes suivantes pour générer la clé SSH :

```
ssh-keygen -t ed25519 -f config/secrets/default.key
```

⚠ Un mot de passe vous sera demandé (passphrase), il faut impérativement le laisser vide.

3.2.10.2 Copier la clé SSH

Lancez les commandes suivantes pour copier la clé SSH sur l'hôte CMC :

```
ssh-copy-id -i config/secrets/default.key user@ip
```

3.2.10.3 Vérifier la connectivité SSH

Lancez la commande suivante pour vérifier la connectivité SSH :

```
ssh -i config/secrets/default.key user@ip_cmc
```

3.2.11 Copier les certificats issus de la PKI

Si le client souhaite intégrer le CMC dans sa PKI, il doit générer le certificat pour le CMC et fournir la clé publique du certificat (cf. 2.2.3 Certificats).

Pour intégrer les éléments issus de la PKI du client, exécutez successivement les commandes suivantes :

```
cp /source/path/cert.key config/secrets/self.cert.key
cp /source/path/cert.pem config/secrets/self.cert.pem
cp /source/path/ca.pem config/secrets/ca.cert.pem
cp /source/path/cert-fullchain.pem
config/secrets/self.fullchain.cert.pem
```

3.2.12 Délégation DNS

Une délégation DNS est nécessaire pour le bon fonctionnement du CMC. Le serveur DNS, autorité du domaine hébergeant le CMC, doit déléguer une sous-zone qui sera gérée directement sur le CMC.

Par exemple, sur le domaine `domaine.lan`, la sous zone `cmc.domaine.lan` est déléguée au serveur DNS interne sur le CMC.

3.2.13 Navigateurs compatibles

Les navigateurs suivants peuvent être utilisés pour exploiter le CMC :

- Chrome ≥ 87 publiée en juillet 2020
- Firefox ≥ 78 publiée en juin 2020
- Safari ≥ 14.1 publiée en avril 2021
- Edge ≥ 88 publiée en janvier 2021

3.3 Machines pilote et CMC

3.3.1 Synchronisation de la date et de l'heure

Les deux machines pilote et CMC doivent être synchronisées en termes de date et d'heure.

3.3.2 Ouverture des flux

Les protocoles suivants doivent être autorisés entre la machine pilote et la machine CMC :

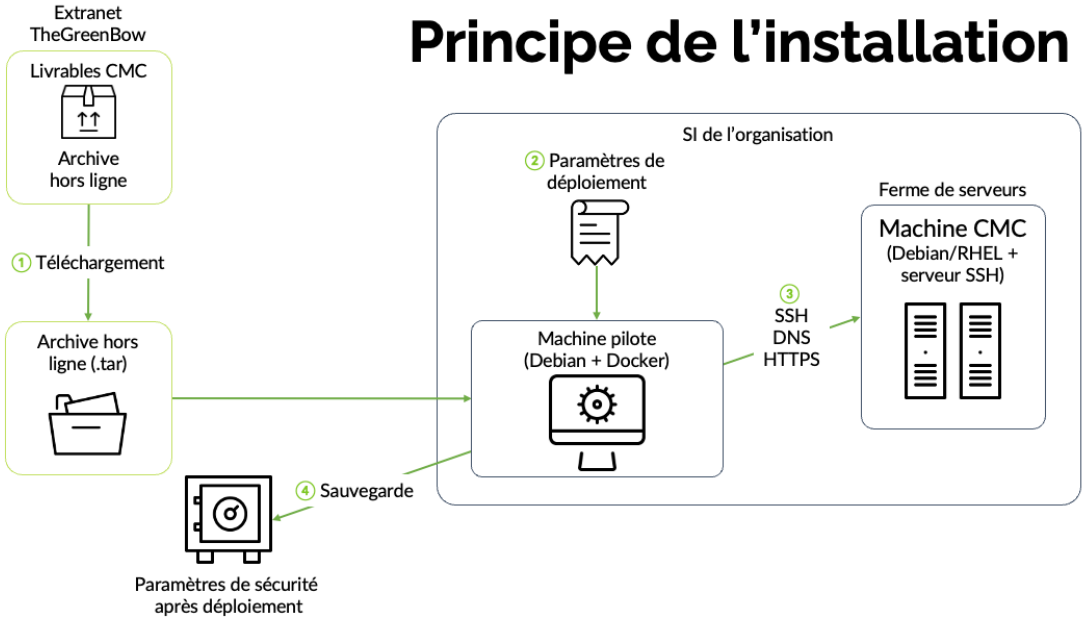
- TCP port 22 (SSH)
- TCP/UDP port 53 (DNS)
- TCP port 443 (HTTPS)

4 Procédure d'installation

4.1 Principe de l'installation

L'installation est prévue pour être réalisée sans accès internet. L'ensemble des packages nécessaires à l'installation (ainsi que leurs dépendances) est embarqué dans l'archive hors ligne.

Afin d'éviter tout problème de dépendances incompatibles, l'ensemble des opérations d'installation est opéré depuis un conteneur Docker.



L'installation du CMC est réalisée au travers d'une machine pilote conformément aux règles de sécurité définies pour le système d'information (SI) de l'organisation. Elle se déroule en quatre étapes simples :

1. Depuis la machine pilote, récupérez l'archive du CMC qui sera déployée sur la machine CMC (serveur de production).
2. Collectez les différents paramètres nécessaires au pilotage de l'installation (certificats, répertoires, nommages, zones réseau, sauvegarde du TAS éventuel, etc.).
3. Poussez le package via SSH depuis la machine pilote vers la machine CMC.
4. À la fin de l'installation, sauvegardez l'ensemble des secrets utilisés au cours de la procédure. Sans cela, il sera impossible d'administrer ultérieurement sur le CMC.

Ces différentes étapes sont décrites plus en détail dans la section suivante.

4.2 Limitations et conditions d'installation

Il est impératif qu'à son état initial la machine CMC corresponde à une installation de base du système d'exploitation, conforme aux prérequis techniques communiqués en amont et validés par le client, et que celle-ci ait subi un minimum de modifications, en particulier en matière de durcissement de la sécurité.

Toute modification préalable du système peut compromettre le bon déroulement de l'installation et des mesures de durcissement prévues. En effet, l'installation intègre déjà des mécanismes de sécurisation, tels que l'interdiction du chargement de modules noyau non utilisés, la désactivation d'IPv6, l'optimisation des paramètres `sysctl`, ainsi que la suppression des paquets inutiles.

⚠ Par conséquent, toute altération préalable du système d'exploitation pourrait entraîner des échecs d'installation et compromettre l'intégrité des configurations de sécurité mises en place.

4.3 Installation hors ligne

Suivre les étapes décrites ci-dessous pour procéder à une installation hors ligne.

Le CMC est hors ligne et ne possède aucun accès internet.

⚠ Il n'est pas possible d'accéder aux dépôts Linux, il convient donc de s'assurer d'avoir installé tous les packages et dépendances requis (cf. section 3.1.5 Dépôts logiciels à jour).

4.3.1 Récupérer l'archive hors ligne

Si cela n'a pas déjà été fait lors de la mise en œuvre des prérequis, il convient de récupérer l'archive hors ligne auprès de l'équipe TGB soit à partir du réseau interne ou à l'aide d'un support amovible. L'image peut être stockée à n'importe quel endroit sur la machine pilote.

☞ Pour plus de détails sur cette opération, voir la section 3.2.4 Rendre disponible l'archive d'installation du CMC.

4.3.2 Contrôles avant installation

4.3.2.1 Dossier inventories

⚠ Pour éviter toute erreur lors de l'installation, il convient de s'assurer que le répertoire `inventories` est bien vide sur la machine pilote.

4.3.2.2 Heure système

⚠ Vérifier que la machine pilote et la machine CMC sont à la même heure.

4.3.2.3 Image instantanée du CMC

⚠ Vous devez impérativement réaliser une image instantanée (ou *snapshot*) de la machine CMC avant de poursuivre l'installation.

4.3.3 Instancier un conteneur de l'installeur

Sur la machine pilote, chargez l'image Docker :

```
docker load < cmc-offline[distribution]-1.3.b.tar.gz
```

Remplacez `[distribution]` par la distribution concernée (`debian` ou `rhel`) et b par le numéro de *build*.

Vérifiez ensuite que l'image est bien chargée :

```
docker images -a

$ docker images -a
REPOSITORY      TAG       IMAGE ID        CREATED       SIZE
cmc-offline     latest    2b5990b523f8    3 days ago    4.6GB
```

L'image `cmc-offline:latest` doit être présente.

Si le TAG n'est pas `latest`, il faut le créer. Voici un exemple de commande :

```
docker tag
gitlab.cmc.thegreenbow.net:5050/cmc/operation-
center/cmc-offline-[distribution]-1.3.b cmc-
offline:latest
```

Remplacez `[distribution]` par la distribution concernée (`debian` ou `rhel`) et b par le numéro de *build*.

⚠ Se placer dans le dossier `instance_cmc` créé lors de la mise en œuvre des prérequis (cf. 3.2.5 Préparation du déploiement), soit au même niveau que le dossier `config`.

Lancer la commande suivante pour instancier un conteneur de l'installeur Docker à partir de l'image :

```
docker run --rm -it \
--mount
type=bind,source="$PWD"/inventories,target=/opt/cmc/inventories
\
--mount type=bind,source="$PWD"/config,target=/opt/cmc/config \
cmc-offline:latest bash
```

4.3.4 Lancer le script d'installation

Exécuter la commande suivante pour lancer le script d'installation :

```
bash entrypoint.sh
```

Le menu d'installation avec les options suivantes s'affiche :

1) Init
2) Install
3) Reboot
4) Stage
5) Management
x) Exit

4.3.5 Lancer Init

Dans le cadre d'une installation hors ligne, l'option Init sert notamment à copier les modules Linux dont on a besoin par la suite.

Pour lancer la commande d'initialisation, entrez 1, puis appuyez sur la touche Entrée.

Suivez les messages qui défilent à l'écran :

- PLAY représente une phase (stage)
- TASK représente une sous-tâche d'un PLAY

Si aucun texte rouge ne s'affiche c'est que l'ensemble des opérations d'initialisation se sont bien déroulées.

Si des messages d'erreur s'affichent en rouge, il convient d'analyser l'origine des erreurs ou contacter le support technique.

4.3.6 Lancer Install

Une fois l'initialisation réalisée, l'installation proprement dite peut être lancée. Pour cela, lorsque le menu d'installation s'affiche, entrez 2, puis appuyez sur la touche Entrée.

Suivez les messages qui défilent à l'écran :

- PLAY représente une phase (stage)
- TASK représente une sous-tâche d'un PLAY

Si aucun texte rouge ne s'affiche c'est que l'ensemble des opérations d'initialisation se sont bien déroulées.

Si des messages d'erreur s'affichent en rouge, il convient d'analyser l'origine des erreurs ou contacter le support technique.

4.3.7 Après l'installation

Avant de réinitialiser la machine pilote, il convient de réaliser plusieurs opérations décrites ci-dessous via l'option de menu **5) Management** du script d'installation (cf. 4.3.4 Lancer le script d'installation).

Lorsque vous sélectionnez cette option, le sous-menu suivant s'affiche :

0) Print secrets
1) Health Check
2) Health Fix
3) Check Config
4) Test installation
99) Go Back to Main Menu
x) Exit

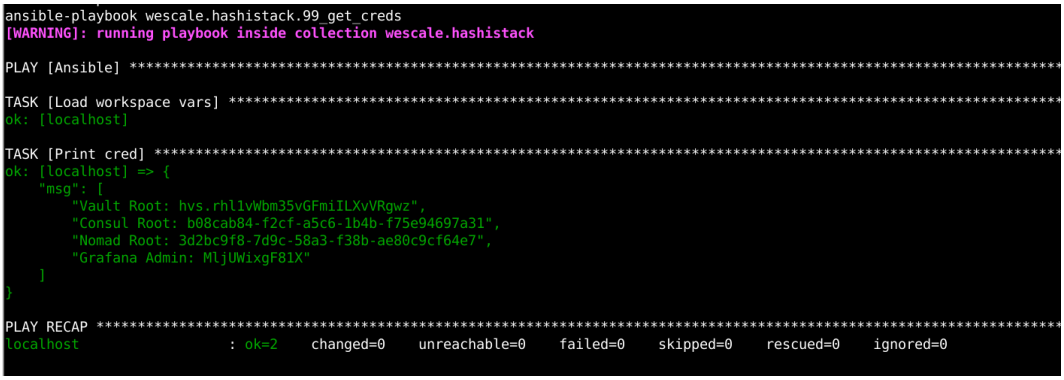
4.3.7.1 Tester l'installation

L'option **4) Test installation** permet de vérifier depuis la machine Pilote si les différents composants du CMC sont fonctionnels.

4.3.7.2 Imprimer les secrets

L'option **0) Print secrets** permet d'afficher les principaux secrets générés pendant le déploiement, à savoir :

- Vault Root : token root pour accéder à Vault
- Consul Root : token root pour accéder à Consul
- Nomad Root : token root pour accéder à Nomad
- Grafana Admin : mot de passe Grafana de l'utilisateur admin



Vous aurez besoin de ces informations pour accéder aux différents conteneurs et services.

☞ Pour savoir comment vous connecter à Grafana, voir la section 7.3 Connexion à Grafana.

4.3.7.3 Sauvegarder l'instance CMC

Le dossier créé à l'issue de l'installation contient les secrets pour accéder aux modules destinés à la maintenance et à la sauvegarde.

Il est donc impératif de sauvegarder l'ensemble du dossier `instance_cmc` sur un support de sauvegarde sécurisé selon vos procédures habituelles.

⚠ Sans ces secrets, plus aucune intervention ne sera possible sur le CMC.

4.3.7.4 Archivage et désarchivage

Après l'installation, il convient de sauvegarder les inventaires :

```
tar cz tar -cz -C inventories | gpg -c -o
config/$cmc_name.tgz.gpg
```

Avant une mise à jour ou une maintenance du CMC, il convient de désarchiver les inventaires :

```
gpg -d config/$cmc_name.tgz.gpg | tar xz -C
/opt/cmc/inventories/
```

4.3.7.5 Essais de bon fonctionnement

Pour tester l'installation, il convient d'ouvrir un navigateur à l'adresse configurée : `cmc.domaine.lan`. Une page de connexion doit s'afficher comme dans la capture d'écran ci-dessous.

Renseignez votre identifiant et votre mot de passe, puis cliquez sur **SE CONNECTER** pour accéder à la page d'accueil du CMC.

Vous disposez de deux comptes utilisateur par défaut dont l'identifiant et le mot de passe figurent dans le tableau ci-dessous :

- un compte d'administrateur,
- un compte d'utilisateur connecté.

Identifiant	Mot de passe
cmc_admin	cmc_admin_pwd
cmc_user	cmc_user_pwd

Il est recommandé de modifier les mots de passe par défaut dès la première connexion. Reportez-vous au Guide de l'administrateur du CMC pour savoir comment procéder.

Consultez les différentes pages et utilisez les fonctions pour vérifier leur bon fonctionnement. Il convient notamment de vérifier que la préparation du TAS s'est bien déroulée.

☞ Pour plus d'informations sur l'utilisation du CMC, reportez-vous au Guide de l'administrateur du CMC.

☞ Pour plus d'informations sur la procédure de préparation du TAS, voir la section 2.2.4 Préparation du TAS.

5 Procédure de redémarrage

Le redémarrage peut s'avérer utile lors de l'ajout de mémoire à une machine physique.

Avant de pouvoir lancer la commande de redémarrage, vous devez disposer de l'archive du dossier `instance_cmc` réalisée en fin d'installation (cf. 4.3.7.4 Archivage et désarchivage).

1. Lancez la commande suivante :

```
docker run --rm -it \
--mount
type=bind,source="$PWD"/inventories,target=/opt/cmc/inventories
\
--mount type=bind,source="$PWD"/config,target=/opt/cmc/config \
cmc-offline:latest
```

2. Lorsque le menu s'affiche, entrez 3, puis appuyez sur la touche Entrée. Cette opération redémarre le CMC et initialise tous les modules.

6 Procédure de restauration

La restauration d'une machine peut s'avérer utile lorsque la machine est plantée ou si vous avez fait une erreur, p. ex. la suppression des configurations.

Le CMC réalise une sauvegarde automatique avec une rétention de 31 jours.

Il est recommandé d'externaliser les sauvegardes afin de pouvoir récupérer des données en cas de panne disque sur le CMC.

7 Gestion de la machine pilote

Il n'est pas indispensable de conserver la machine pilote dans son état à l'issue de l'installation. Toutefois, il est impératif de conserver l'image Docker et les secrets (cf. 4.3.7.3 Sauvegarder l'instance CMC).

7.1 Désarchivage des inventaires

Avant de procéder à une mise à jour ou à des opérations de maintenance du CMC, vous devez désarchiver vos inventaires. Reportez-vous à la section 4.3.7.4 Archivage et désarchivage pour savoir comment procéder.

7.2 Menu de gestion du CMC

L'option de menu **5) Management** du script d'installation (cf. 4.3.4 Lancer le script d'installation) sert à réaliser un contrôle sanitaire du serveur et des secrets.

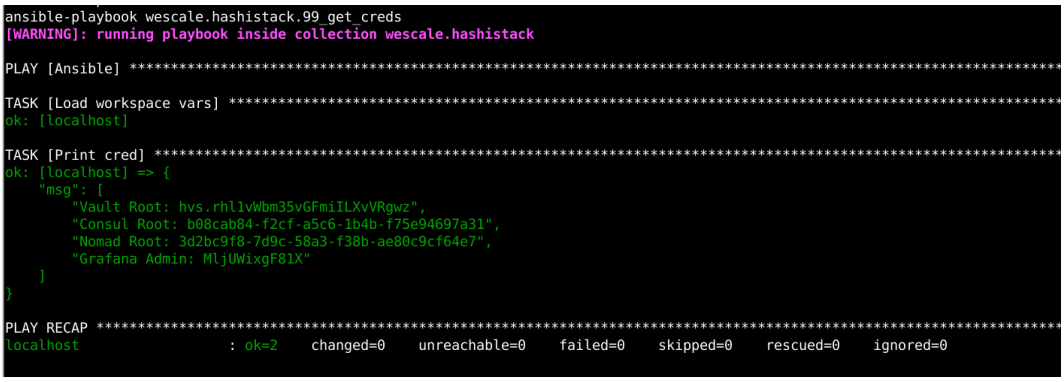
Lorsque vous sélectionnez cette option, le sous-menu suivant s'affiche :

0) Print secrets
1) Health Check
2) Health Fix
3) Check Config
4) Test installation
99) Go Back to Main Menu
x) Exit

7.2.1 Imprimer les secrets

L'option **0) Print secrets** permet d'afficher les principaux secrets générés pendant le déploiement, à savoir :

- Vault Root : token root pour accéder à Vault
- Consul Root : token root pour accéder à Consul
- Nomad Root : token root pour accéder à Nomad
- Grafana Admin : mot de passe Grafana de l'utilisateur admin



Vous aurez besoin de ces informations pour accéder aux différents conteneurs et services.

☞ Pour savoir comment vous connecter à Grafana, voir la section 7.3 Connexion à Grafana.

7.2.2 Contrôle sanitaire

L'option **1) Health Check** lance une vérification des fonctions « vitales » du CMC.

Les services suivants sont contrôlés :

- point d'accès admin du CMC ;
- service de tableau de bord des logs ;
- point d'accès de la remontée des logs ;
- services métiers (TAS, éditeur de configuration) ;
- services du socle d'exécution (authentification, maillage de services [ou *service mesh* en anglais], orchestrateur de services métiers).

7.2.3 Correctif sanitaire

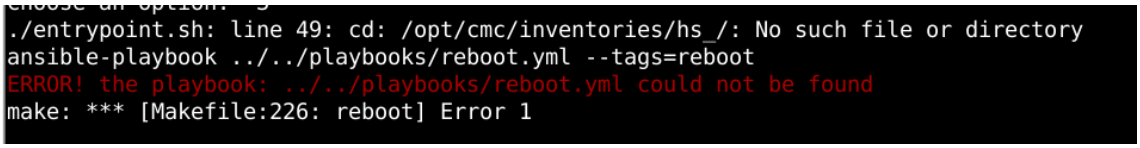
L'option **2) Health Fix** redémarre les fonctions « vitales » du CMC.

7.2.4 Contrôle de la configuration

L'option **3) Check config** permet de vérifier les éléments suivants avant déploiement :

- le fichier `config.yml` existe ;
- la clé privée ssh `default.key` existe dans `config/secrets` ;
- la clé publique ssh `default.key.pub` existe dans `config/secrets`.

Exemple de message d'erreur retourné lorsqu'une anomalie est détectée :



7.3 Connexion à Grafana

Pour vous connecter à Grafana, procédez comme suit :

1. Lancez le script d'installation (cf. 4.3.4 Lancer le script d'installation).
2. Sélectionnez l'option **5) Management**.
3. Sélectionnez l'option **0) Print secrets**.
4. Notez le mot de passe indiqué après Grafana Admin.
5. Ouvrez un navigateur et accédez à l'URL de Grafana : `grafana.cmc.domaine.lan`.
6. Indiquez comme nom d'utilisateur : `admin`.
7. Utilisez le mot de passe noté à l'étape 4.

Vous pouvez utiliser Grafana pour générer des tableaux de bord à afficher dans la partie **Supervision** du CMC.

7.4 Mise à jour du système

⚠ Les administrateurs du CMC ne doivent pas gérer eux-mêmes les mises à jour métier ou des paquets, qu'il s'agisse du système d'exploitation ou de la pile de services HashiStack au cœur du produit.

Le CMC est constitué d'un ensemble de logiciels qui correspond à une version précise du système d'exploitation sous-jacent installé sur la machine CMC. En cas d'évolution du produit, du système d'exploitation ou de la pile HashiStack, ou en cas de détection d'une CVE, la mise à jour doit obligatoirement se faire à l'aide de l'installeur sur la machine pilote et avec l'assistance du support technique TheGreenBow.

☞ Pour savoir comment contacter le support technique, reportez-vous à la section 8.3 Support.

8 Contact

8.1 Information

Toutes les informations sur les produits TheGreenBow sont disponibles sur le site : https://thegreenbow.com/.

8.2 Commercial

Contact téléphonique : +33.1.43.12.39.30

Contact mail : sales@thegreenbow.com

8.3 Support

Le site TheGreenBow propose plusieurs pages concernant le support technique des logiciels :

Aide en ligne

https://thegreenbow.com/fr/support/assistance/

FAQ

https://thegreenbow.com/fr/faq/

Formulaire de contact

Le support technique est accessible via un formulaire disponible sur le site TheGreenBow à l'adresse : https://thegreenbow.com/fr/support/assistance/support-technique/.

Vos connexions protégées
en toutes circonstances

28, rue Caumartin
75009 Paris – France

sales@thegreenbow.com

www.thegreenbow.com