réseaux & iut télécoms St-Malo

Université de Rennes

Rapport de test du projet

Application de collecte d'informations sur les machines d'infrastructure

by

Théo Da Conceicao

Thomas Chevalier

Alban Burlot

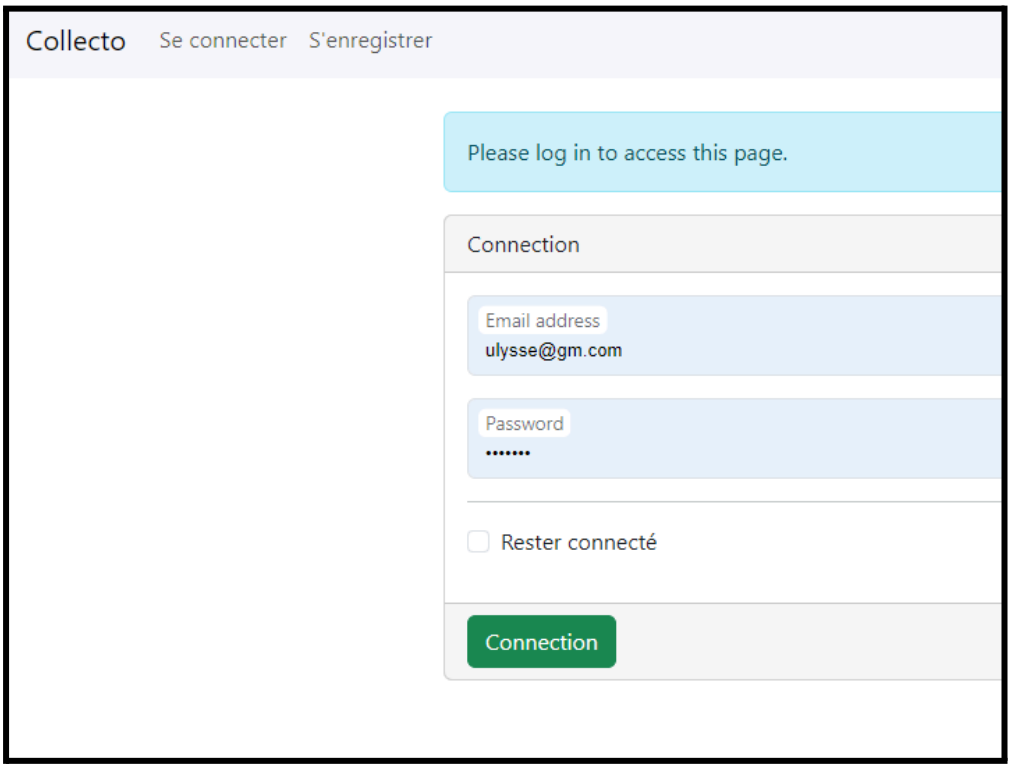
Lucas Bunel

Ulysse Parmentier

Sommaire

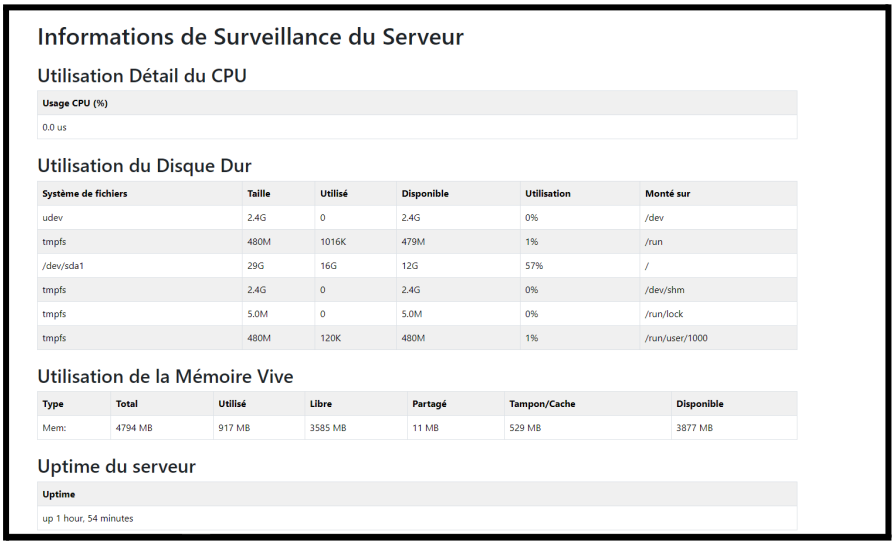
II - Connexion à Collecto

Ci-dessous sont renseignés l'ensemble des tests vérifiant l'ensemble des fonctionnalités de Collecto. L'utilisateur renseigne son adresse e-mail et son mot de passe après s'être crée un compte dans l'onglet "S'enregistrer".



II - Visualisation des données (Accueil)

Ce dernier arrive ensuite à l'accueil du site lui permettant de visualiser les différentes statistiques (utilisation disque dur, RAM, etc) concernant sa machine :



III - Visualisation des données (Audits de sécurité)

Dans l'onglet "Audits de sécurité", des informations sont visibles tels que l'état des ports ouverts, les processus SSH ainsi que les logs (nous avons ici pris trois services : ssh, apache2 et les journaux de boot).
Sur la VM voici la sortie lorsque l'on souhaite voir les ports ouverts :

```
└─$ netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
```

Les processus tournant en arrière plan :

```
┌──(user㉿kali)-[/var/log]
└─$ ps -aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.2  21384 12776 ?        Ss   10:39   0:02 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    10:39   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   10:39   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   10:39   0:00 [rcu_par_gp]
root           5  0.0  0.0      0     0 ?        I<   10:39   0:00 [slub_flushwq]
root           6  0.0  0.0      0     0 ?        I<   10:39   0:00 [netns]
root           8  0.0  0.0      0     0 ?        I<   10:39   0:00 [kworker/0:0H-events_highpri
root          11  0.0  0.0      0     0 ?        I<   10:39   0:00 [mm_percpu_wq]
root          12  0.0  0.0      0     0 ?        I    10:39   0:00 [rcu_tasks_kthread]
root          13  0.0  0.0      0     0 ?        I    10:39   0:00 [rcu_tasks_rude_kthread]
```

Et l'affichage de ces données dans collecto (colonne utilisateur, nom de processus et PID) :

État des ports

Search:

Numéro de port	Nom du port ouvert	État
79	Autre	CLOSED
80	HTTP	OPEN
81	Autre	CLOSED

Showing 1 to 3 of 3 entries

Previous 1 Next

Processus SSH

Search:

Utilisateur	Nom du processus	PID	CPU %
colord	/usr/libexec/colord	1190	
message+	/usr/bin/dbus-daemon	523	
polkitd	/usr/lib/polkit-1/polkitd	528	
root	/sbin/init	1	
root	[kthreadd]	2	
root	[rcu_gp]	3	
root	[rcu_par_gp]	4	
root	[slub_flushwq]	5	
root	[netns]	6	

Il reste enfin la visualisation des logs :

Logs de démarrage sur la kali:

```
┌──(user㉿kali)-[/var/log]
└─$ dmesg | tail -n 50
[  792.085656] [drm:vmw_msg_ioctl [vmwgfx]] *ERROR* Failed to open channel.
[  792.085697] [drm:vmw_msg_ioctl [vmwgfx]] *ERROR* Failed to open channel.
[  793.403719] [drm:vmw_msg_ioctl [vmwgfx]] *ERROR* Failed to open channel.
[  793.403766] [drm:vmw_msg_ioctl [vmwgfx]] *ERROR* Failed to open channel.
[  793.408880] [drm:vmw_msg_ioctl [vmwgfx]] *ERROR* Failed to open channel.
[  793.408920] [drm:vmw_msg_ioctl [vmwgfx]] *ERROR* Failed to open channel.
[  795.394064] [drm:vmw_msg_ioctl [vmwgfx]] *ERROR* Failed to open channel.
[  795.394103] [drm:vmw_msg_ioctl [vmwgfx]] *ERROR* Failed to open channel.
[ 1783.081271] ohci-pci 0000:00:06.0: frame counter not updating; disabled
[ 1783.081280] ohci-pci 0000:00:06.0: HC died; cleaning up
[ 1783.082347] usb 2-1: USB disconnect, device number 2
[ 5517.263320] watchdog: BUG: soft lockup - CPU#0 stuck for 248s! [swapper/0:0]
[ 5517.263350] Modules linked in: snd_seq_dummy snd_hrtimer snd_seq snd_seq_device
soundcore vboxguest ac sg serio_raw evdev binfmt_misc fuse dm_mod configfs loop efi
ntel sha512_ssse3 sr_mod cdrom crc64_rocksoft_generic ata_generic sha512_generic cr
ohci_pci ohci_hcd aesni_intel ehci_pci crypto_simd ehci_hcd psmouse cryptd e1000 i2
[ 5517.264216] CPU: 0 PID: 0 Comm: swapper/0 Tainted: G        W          6.5.0-kal
[ 5517.264233] Hardware name: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 1
[ 5517.264240] RIP: 0010:pv_native_safe_halt+0×f/0×20
[ 5517.264277] Code: 0b 66 2e 0f 1f 84 00 00 00 00 00 90 90 90 90 90 90 90 90 90 90
[ 5517.264284] RSP: 0018:ffffffffba003e80 EFLAGS: 00010296
[ 5517.264294] RAX: 0000000000000000 RBX: 0000000000000000 RCX: 0000000000000000
[ 5517.264300] RDX: 4000000000000000 RSI: ffffffffb9850a42 RDI: ffffffffb983cffe
[ 5517.264305] RBP: ffffffffba010900 R08: 0000000000000001 R09: 0000000000000000
[ 5517.264310] R10: 0000000000000026 R11: 0000000000000000 R12: 0000000000000000
[ 5517.264315] R13: 0000000000000000 R14: ffffffffba010900 R15: 0000000000000000
[ 5517.264321] FS:  0000000000000000(0000) GS:ffff9f5513400000(0000) knlGS:00000000
[ 5517.264328] CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
[ 5517.264333] CR2: 00007f028efafc3c CR3: 00000001199f4004 CR4: 00000000000306f0
[ 5517.264345] Call Trace:
```

Logs d'apache2…

```
┌──(user㉿kali)-[~]
└─$ tail -n 50 /var/log/apache2/access.log
::1 - - [02/Feb/2024:12:30:21 +0100] "GET / HTTP/1.1" 200 10956 "-" "curl/8.4.0"
```

…qui sont eux aussi visibles à fin de la page :