12/10/2025 05:03 1/6 Création d'un nouveau service

Création d'un nouveau service



Heimdall & Grydur éteints donc c'est obsolète. Il y a juste la fin qui est intéressant : créer son petit logo/texte pour le motd

Bon, il y a normalement tout en place pour mettre en place facilement de nouveaux services. Chaque service va dans une Jail. Et on essaye de faire propre et épuré dans une jail. Pas besoin de vim ou bash (normalement).

Où?

Sur Heimdall ou Grydur. Ce sont des machines FreeBSD avec des gros disques ZFS. Donc faites pour servir!

Vous pouvez aussi essayer d'utiliser frigg, mais elle est nettement moins puissante et n'a pas de disques ZFS.

Attends, je pige rien

Lis ça et ça

Envoie la sauce, I am ready!

On respecte les conventions :

	heimdall	grydur	
IP pour les jails	10.3.15.50 à 10.3.15.99	10.3.15.100 à 10.3.15.149	

On ne choisit évidemment pas une IP qui a déjà été prise...

Exemple sur heimdall:

```
root@heimdall ~ # jls # on vérifie qu'on va pas faire n'importe quoi
       IP Address
   JID
                         Hostname
                                                        Path
     1
        10.3.15.50
                         samba
                                                        /jail/samba
     2
        10.3.15.56
                                                        /jail/pxe
                         pxe
     4
       10.3.15.59
                         graphite
                                                        /jail/graphite
     5
        10.3.15.60
                         grafana
                                                        /jail/grafana
     6
        10.3.15.58
                         duplicity
                                                        /jail/duplicity
     7
        10.3.15.57
                         ck-mirror
                                                        /jail/ck-mirror
     8
        10.3.15.53
                         bounce
                                                        /jail/bounce
     9
        10.3.15.54
                         ldap
                                                        /jail/ldap
# # l'interface réseau pour heimdall est bge0
# # SAUF ACCORD EXPLICITE DU CRI, pour grydur, c'est em0; si tu mets bge0,
```

```
tu vas TOUT niquer sur le réseau ext.ec-m.fr
root@server# ezjail-admin create
ma_nouvelle_jail_avec_un_nom_explicite_et_court
'mon_interface_réseau|10.3.15.XY'
root@server# ezjail-admin start
ma_nouvelle_jail_avec_un_nom_explicite_et_court
# # blah blah...
```

Et sur Grydur:

root@grydur ~ (git)-[master] # jls				
JID	IP Address	Hostname	Path	
1	10.3.15.105	terraria	/jail/terraria	
2	10.3.15.100	phytv	/jail/phytv	
3	10.3.15.106	owncloud	/jail/owncloud	
4	10.3.15.108	openra	/jail/openra	
5	10.3.15.104	nagios	/jail/nagios	
6	10.3.15.107	mysql	/jail/mysql	
7	10.3.15.103	minecraft	/jail/minecraft	
8	10.3.15.101	jenkins	/jail/jenkins	
9	10.3.15.102	gitlab	/jail/gitlab	

Voilà, une jail. Toute propre, tout bien :)

OK, j'ai une jail, now what?

Avant toute chose

On prend un instantané¹⁾ ZFS:

```
root@serveur# zfs snapshot jail/ma_jail@"$(date +%Y-%m-%d)"
```

PKG managment



Interdiction d'utiliser pkg directement dans la jail

MAJ

Bah il y a une FreeBSD dedans. Donc on en prend soin. Une idée, c'est par exemple de la mettre à jour.

```
root@serveur# pkg -j ma_jail upgrade
root@serveur# ezjail-admin restart ma_jail
```

12/10/2025 05:03 3/6 Création d'un nouveau service

Et on s'assure n'avoir rien pété... on regarde le nagios, par exemple. S'il y a une application web sur la machine, on s'assure qu'elle fonctionne encore, etc.

Installation de choses

On upgrade, d'abord. Puis ensuite :

root@serveur# pkg -j ma_jail install mon_paquet

C'est bien mignon, mais là, j'ai pas encore mis les pieds dans ma jail !



Si tu as déjà eu le prompt root@ma_jail#, je propose que tu te suicides ou au moins que tu arrêtes le sysadmin

root@serveur# ezjail-admin console ma_jail
MOTD...
root@ma_jail#

Voilà, tu as ta jail. Tu peux jouer avec comme avec un serveur normal à l'exception de **ne pas utiliser pkg dedans**

On configure et on fait tourner son service...

Tu te débrouilles, c'est maintenant qu'intervient ta matière grise.



Si un service étrange tourne en tant qu'un utilisateur que **tu** as créé de toutes pièces (genre le user openra dans la jail openra). Il est impératif de mettre son shell à /sbin/nologin pour éviter qu'une faille dans le logiciel ne permette à un pirate de mettre les pieds dans la jail.

Tests

Avant de continuer et de le mettre en wide-open sur le réseau, on teste le service depuis Sif (Genre au pif, check_tcp).

On écrit les tests (sur sif) pour la nouvelle jail qui sera ajoutée aux machines :

/usr/local/etc/nagios/objects/ginfo/hosts.cfg

define host{

/usr/local/etc/nagios/objects/ginfo/services.cfg

Pare-Feu

Avec tes petits neurones maintenant, tu décides qui a le droit d'accès vers ton service. Puis sur odin... bah on fait de la conf pf !

/etc/pf.conf

```
# Machines
# [...]
ma_jail=10.3.15.XY
mon_super_port=11111
# [...]

# Mon super service du feu
pass in quick inet proto tcp from <local> to $ma_jail port
$mon_super_port
# [...]
```

Tu peux aussi utiliser les tables existantes, au besoin... après avoir usé de tes neurones!

OK, et pour le luiz

Un zoli MOTD

12/10/2025 05:03 5/6 Création d'un nouveau service

Générique : Dans /etc/motd, mettez le texte "Ma jail" en ascii art en fonte "graffiti" ici

Moins générique : Un truc plus original

Exemples

/jail/gitlab/etc/motd

/jail/openra/etc/motd

```
FreeBSD 10.1-RELEASE-p6 (GENERIC) #0: Tue Feb 24 19:00:21 UTC 2015
                 !########
                                  #
               !######!
                                   ##!
            !######!
                                     ###
         !#########
                                      ####
                                      ######
      #############
        !###!
                   !####!
                                       ######
                                       #####!
                      #####
                        !####!
                                       #######
                           #####
                                       #######
                                      ######!
                             !####!
                                ####!#######
            ##
                                  ##########
           ,#####!
                             !###########
         ,#### ######################!
       ,####'
                  ######### ! '
                                          #####
     ,####
                       #######
                                            !####!
   #### '
                                               #####
   ~##
                                                 ##~
              Welcome back, commander.
```

qu'il est moche ce mot français...

From:

https://wiki.centrale-med.fr/ginfo/ - Wiki GInfo

Permanent link:

https://wiki.centrale-med.fr/ginfo/musee:nouveau

Last update: 26/01/2017 13:41

