**Palier système linux EL 7 (7.1.0) – PTE Réseau**

Conventions typographiques

Les conventions suivantes sont utilisées dans la suite du document :

* les commandes à taper dans un terminal sont indiquées dans un cadre :

# uname -a

Linux nom.domaine 2.6.18-164.el5 #1 SMP Tue Aug 18 15:51:48 EDT 2009 x86\_64 x86\_64 x86\_64 GNU/Linux

* les extraits de fichiers utilisent la même convention :

UsePrivilegeSeparation yes

* une note informative utilise le formalisme suivant :

|  |  |
| --- | --- |
|  | L’invite $ devant une commande indique qu’elle peut être exécutée par un utilisateur non privilégié |

* un avertissement indique un risque, et est présenté ainsi :

|  |  |
| --- | --- |
|  | L’invite # devant une commande indique qu’elle doit être exécutée en tant qu’utilisateur privilégié[[1]](#footnote-1). |

* les points d’attention sont en surbrillance dans le texte ;
* les termes techniques tels que cat sont signalés par une fonte à chasse fixe.

Assistance

Le support du système de référence est assuré par :

[dsp-cspito-support-serveurs@edf.fr](mailto:dsp-cspito-support-serveurs@edf.fr)

(cellule de support SCOPE : I\_ING\_SUPPORT-SERVEURS\_SN3)

(cellule de support POGS : ITO\_ING\_SUPPORT-SERVEURS\_SN3)

Merci d’utiliser exclusivement ce circuit pour vos demandes d’assistance.

Remarques

Si vous constatez une erreur, ambiguïté, manque de clarté, ou si vous avez une amélioration à suggérer sur ce document, merci d’écrire à :

[**dsp-cspito-ing-srv-linux@edf.fr**](mailto:dsp-cspito-ing-srv-linux@edf.fr?subject=Remarque%20sur%20le%20document%20:)

Cette adresse n’est pas une boite de support.

Contenu

1 Opérations réseau 5

1.1 Etat des interfaces 5

1.1.1 Adressage 5

1.1.2 Etat des liens réseaux 6

1.1.3 Afficher la Passerelle par défaut 7

1.2 Configuration des interfaces 7

1.3 Configuration du réseau 8

1.4 Configuration manuelle des interfaces 9

1.4.1 Adressage 9

1.4.2 Création IP virtuelle 9

1.4.3 Activation / Désactivation 9

1.4.4 Configuration de la passerelle 9

1.5 Dénomination des machines 10

1.6 Identifier une machine 10

1.7 Synchronisation NTP 11

1.8 Dé-bridage des ports réseaux 12

1.9 Fichier /etc/services 13

2 Pare-Feu (Firewall) 14

2.1 Description 14

2.2 Principe 14

2.3 Pré-requis 14

2.4 Opérations sur le pare-feu 15

2.4.1 Afficher les règles du pare-feu 15

2.4.2 Démarrage du service 16

2.4.3 Arrêt du service 16

2.4.4 Relance du service 16

2.4.5 Désactivation du Pare-Feu (uniquement sur une souche N1) 16

2.4.6 Ajout d’une règle 17

2.4.7 Sauvegarde de la configuration du pare-feu 18

2.4.8 Retrait d’une règle 18

3 Multi-attachement réseau 20

3.1 Redondance avec tolérance de panne simple 20

3.1.1 Principe 20

3.1.2 Pré-requis 20

3.1.3 Opérations à effectuer 21

3.1.3.1 Module noyau bonding 21

3.1.3.2 Fichier /etc/sysconfig/network-scripts/ifcfg-<interface> 21

3.1.3.3 Réactivation des interfaces réseau et redémarrage du service réseau 22

3.1.4 Vérification de la mise en place 23

4 Bibliographie 26

# Opérations réseau

## Etat des interfaces

### Adressage

Pour afficher l’état du réseau d’une machine, utilisez la commande suivante :

# ip addr show

1: lo: <LOOPBACK,UP,LOWER\_UP> mtu 65536 qdisc noqueue state UNKNOWN

link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00

inet 127.0.0.1/8 scope host lo

valid\_lft forever preferred\_lft forever

2: ens32: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc pfifo\_fast state UP qlen 1000

link/ether <Adresse MAC> brd ff:ff:ff:ff:ff:ff

inet <Adresse IP>/<Masque de sous réseau> brd <Broadcast> scope global ens32

valid\_lft forever preferred\_lft forever

Les éléments surlignés permettent de récupérer les principales informations d’une interface.

Les interfaces sont nommées « en\*X » ou X est le numéro de l’interface.

lo est l’interface dite de loopback, qui permet au serveur de communiquer en local.

|  |  |
| --- | --- |
|  | La commande ifconfig fonctionne pour des raisons de compatibilité. Il est conseillé d’utiliser la commande ip qui remplace ifconfig |

# ifconfig

ens32: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet :<Adresse IP> netmask <Masque de sous réseau> broadcast <Broadcast>

ether <Adresse MAC> txqueuelen 1000 (Ethernet)

RX packets 18725 bytes 6005050 (5.7 MiB)

RX errors 0 dropped 912 overruns 0 frame 0

TX packets 3788 bytes 458260 (447.5 KiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536

inet 127.0.0.1 netmask 255.0.0.0

loop txqueuelen 0 (Local Loopback)

RX packets 12 bytes 852 (852.0 B)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 12 bytes 852 (852.0 B)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

|  |  |
| --- | --- |
|  | La commande ifconfig fonctionne pour des raisons de compatibilité. Il est conseillé d’utiliser la commande ip qui remplace ifconfig |

Pour récupérer l’interface par défaut :

# ip route list | awk '/^default/ {print $NF}'

ens32

L’adresse IP par défaut :

# DEFDEV=$(ip route list | awk '/^default/ {print $NF}')

# ip addr show $DEFDEV | grep inet | grep -v inet6 | awk '{print $2}' | awk -F/ '{print $1}'

10.122.26.34

### Etat des liens réseaux

Pour afficher l’état des liens réseaux, veuillez taper la commande suivante :

# ethtool ens32

Settings for ens32:

Supported ports: [ TP ]

Supported link modes: 10baseT/Half 10baseT/Full

100baseT/Half 100baseT/Full

1000baseT/Full

Supported pause frame use: No

Supports auto-negotiation: Yes

Advertised link modes: 10baseT/Half 10baseT/Full

100baseT/Half 100baseT/Full

1000baseT/Full

Advertised pause frame use: No

Advertised auto-negotiation: Yes

Speed: 1000Mb/s

Duplex: Full

Port: Twisted Pair

PHYAD: 0

Transceiver: internal

Auto-negotiation: on

MDI-X: off (auto)

Supports Wake-on: d

Wake-on: d

Current message level: 0x00000007 (7)

drv probe link

Link detected: yes

Dans le cas ou vous voulez récupérer les informations de votre interface « ens32 ».

Vous pouvez récupérer via les informations surlignées :

* La vitesse du lien en cours : Speed
* L’activation ou non de l’auto-negotiation : Auto-negotiation
* L’état du lien : Link detected
* Ainsi que les vitesses supportées par la carte : Supported link modes

### Afficher la Passerelle par défaut

Pour afficher la passerelle configurée :

# ip route list | awk '/^default/ {print $3}'

10.122.26.3

## Configuration des interfaces

Il existe des fichiers de configuration permettant de configurer les interfaces réseaux automatiquement à chaque démarrage.

Ceux-ci se situent dans le répertoire : /etc/sysconfig/network-scripts

Ils se nomment ifcfg-en\*X ou X est le numéro de l’interface.

Il est composé des lignes suivantes :

NAME="ens32"

DEVICE="ens32"

ONBOOT=yes

NETBOOT=yes

UUID="6333434d-689e-46ee-89b5-b0e06059fb3f"

IPV6INIT=no

BOOTPROTO=none

TYPE=Ethernet

DEFROUTE=yes

IPV4\_FAILURE\_FATAL=no

IPADDR=<adresse IP>

PREFIX=<Masque de sous réseau au format XX>

GATEWAY=<Adresse IP de la passerelle par defaut>

La ligne ONBOOT active ou non l’interface au démarrage de la machine.

La ligne BOOTPROTO défini si l’interface a une adresse IP statique (none) ou fournie par le serveur (dhcp).

La ligne IPADDR défini l’adresse IP de l’interface.

La ligne PREFIX défini le masque réseau de l’interface au format XX (exemple PREFIX=24).

La ligne GATEWAY défini l’adresse IP de la passerelle par défaut.

## Configuration du réseau

Le fichier /etc/sysconfig/network définit les paramètres réseaux globaux au niveau du système.

|  |  |
| --- | --- |
|  | L’installeur Rhel7 renseigne le fichier d’interface /etc/sysconfig/network-scripts/ifcfg-enX et laisse vide le fichier /etc/sysconfig/network |

Ce fichier permet un certain nombre de choses, notamment l’activation / désactivation du réseau complet sur la machine, l’activation / désactivation de l’IPV6, la configuration de la passerelle par défaut et la configuration du nom de la machine.

Pour configurer la passerelle par défaut il suffit de modifier la ligne GATEWAY si elle existe ou de l’ajouter :

GATEWAY= <Adresse IP de la passerelle par defaut>

NETWORKING=yes

HOSTNAME=<FQDN du Serveur>

NOZEROCONF=yes

## Configuration manuelle des interfaces

### Adressage

La configuration des interfaces peut se faire également via les commandes ip ou ifconfig.

# ip addr add <ip>/<masque de sous réseau au format XX> dev <interface>

# ifconfig <interface> inet <ip> netmask <masque de sous reseau>

La commande suivante permet de calculer le masque de sous réseau au format XX (prefix) :

# ipcalc -np <ip> <masque de sous reseau>

PREFIX=24

NETWORK=10.122.26.0

Pour un netmask de 255.255.255.0 le netmask au format XX (prefix) est **24**

### Création IP virtuelle

Pour créer des IP virtuelles il suffit d’ajouter à l’interface choisie « :X » ou X est le chiffre de votre choix.

# ifconfig <interface>:X inet <ip> netmask <masque de sous reseau>

### Activation / Désactivation

Pour activer l’interface réseau :

# ifup <interface>

Pour désactiver l’interface réseau :

# ifdown <interface>

### Configuration de la passerelle

Pour configurer la passerelle par défaut :

# ip route add default via <ip de la passerelle>

## Dénomination des machines

Le nom des machines se configure dans le fichier : /etc/hostname qui contient une ligne avec le hostname long :

<nom long de la machine>

Le nom long (FQDN) est composé de la façon suivante :

<nom court de la machine>.<3 lettres du site ou se situe la machine>.<domaine edf> .

Se référer au document CSP-IT-SRT-DISIS-DOC-10-074 concernant le nommage des machines.

|  |  |
| --- | --- |
|  | Il est impératif d’utiliser le nom long (FQDN) ! |

Pour fixer le hostname il est pratique d’utiliser la commande suivante :

# hostnamectl set-hostname <nom long de la machine>

Pour s’assurer que le hostname a bien été fixé la commande suivante est nécessaire :

# hostnamectl status

## Identifier une machine

Pour connaitre l’adresse IP depuis le nom d’une machine, ou l’inverse, il suffit d’utiliser la commande :

# host <nom de la machine ou adresse IP>

claytest.cla.edfgdf.fr is an alias for cla02test.cla.edfgdf.fr.

cla02test.cla.edfgdf.fr has address 10.0.0.1

## Synchronisation NTP

Lorsque l’installation a été réalisée par SIP/SIR, le paramétrage du service ntp est déjà opérationnel. Voici quelques éléments permettant de s’assurer que le service est bien actif.

Lorsque le service vient d’être démarré :

# ntpstat

unsynchronised

time server re-starting

polling server every 64 s

Après quelques minutes, la synchronisation devrait être effective :

# ntpstat

synchronised to NTP server (192.168.126.254) at stratum 8

time correct to within 489 ms

polling server every 64 s

Pour vérifier la liste des serveurs de temps utilisés :

# ntpq -np

remote refid st t when poll reach delay offset jitter

==============================================================================

\*192.168.126.254 10.50.49.245 7 u 35 64 177 3.096 -0.908 0.641

+192.168.127.254 10.50.49.241 7 u 33 64 177 3.042 -0.520 0.530

## Dé-bridage des ports réseaux

|  |  |
| --- | --- |
|  | Ce paragraphe s’applique aux machines physiques (rien n’est à faire sur les VM) |

SRT ne garantit pas l’auto-négociation de ses commutateurs.

Si jamais vous avez obtenu un port réseau gigabit non bridé, voici la procédure à suivre pour débrider les interfaces réseaux après installation si cela est nécessaire.

Récupérer la liste des interfaces réseaux :

$ ls -l /etc/sysconfig/network-scripts/ifcfg-en\*

-rw-r--r-- 1 root root 326 Jul 3 16:47 /etc/sysconfig/network-scripts/ifcfg-eno1

-rw-r--r--. 1 root root 270 Jul 3 16:15 /etc/sysconfig/network-scripts/ifcfg-eno2

Pour chacun des fichiers indiqués, vérifier qu’il n’y a pas de ligne *ETHTOOL\_OPTS* avec l’option autoneg off par exemple :

ETHTOOL\_OPTS="autoneg off speed 100 duplex full"

Si la ligne est présente, la remplacer par la ligne suivante :

ETHTOOL\_OPTS="autoneg on"

Redémarrer le service réseau :

# service network restart

Restarting network (via systemctl): [ OK ]

Vos interfaces réseaux doivent maintenant être en auto-négociation :

# ethtool eno1

Settings for eno1:

Supported ports: [ TP ]

Supported link modes: 10baseT/Half 10baseT/Full

100baseT/Half 100baseT/Full

1000baseT/Full

Supported pause frame use: No

Supports auto-negotiation: Yes

Advertised link modes: 10baseT/Half 10baseT/Full

100baseT/Half 100baseT/Full

1000baseT/Full

Advertised pause frame use: No

Advertised auto-negotiation: Yes

Speed: 1000Mb/s

Duplex: Full

Port: Twisted Pair

PHYAD: 0

Transceiver: internal

Auto-negotiation: on

MDI-X: off (auto)

Supports Wake-on: d

Wake-on: d

Current message level: 0x00000007 (7)

drv probe link

Link detected: yes

## Fichier /etc/services

Le fichier /etc/services permet de connaitre la correspondance des ports par défaut en fonction du service.

|  |  |
| --- | --- |
|  | Il ne faut en aucun cas modifier le fichier /etc/services. |

# Pare-Feu (Firewall)

## Description

Un pare-feu logiciel est un logiciel permettant de contrôler les communications réseaux. Il permet donc de faire respecter un politique de sécurité réseau concernant les accès à une ressource réseau.

Ce contrôle des communications peut être effectué par application (ou service) ou par paquet.

## Principe

Il a pour principale tâche de contrôler le trafic entre différentes zones de confiance, en filtrant les flux de données qui y transitent.

Le filtrage ou règle se fait selon divers critères. Les plus courants sont :

* l'origine ou la destination des paquets (adresse IP, ports TCP ou UDP, interface réseau, etc.)
* les options contenues dans les données (fragmentation, validité, etc.)
* les données elles-mêmes (taille, correspondance à un motif, etc.)

Les règles du pare-feu sont exécutées séquentiellement. L’ordre des règles est donc très important.

La configuration par défaut du pare-feu sur la souche RHEL7 permet le trafic sortant mais filtre le trafic entrant. Seul le service SSH est ouvert afin de permettre les connexions sur le serveur.

## Pré-requis

Tous les pré-requis au fonctionnement du pare-feu sont présents et fonctionnels à partir de la souche EDF RedHat 6.

Il a été décidé que le Pare-feu (Firewall) pourrait dorénavant être désactivé sur une **souche N1**.

## Opérations sur le pare-feu

### Afficher les règles du pare-feu

La commande permettant d’afficher les règles du pare-feu :

# iptables -L

Chain INPUT (policy ACCEPT)

target prot opt source destination

ACCEPT all -- anywhere anywhere state RELATED,ESTABLISHED

ACCEPT icmp -- anywhere anywhere

ACCEPT all -- anywhere anywhere

ACCEPT tcp -- anywhere anywhere state NEW tcp dpt:ssh

ACCEPT tcp -- anywhere anywhere state NEW tcp dpt:51234

ACCEPT udp -- anywhere anywhere state NEW udp dpt:ntp

ACCEPT tcp -- anywhere anywhere state NEW tcp dpt:ntp

REJECT all -- anywhere anywhere reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)

target prot opt source destination

REJECT all -- anywhere anywhere reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)

target prot opt source destination

Si le service iptables est arrété, le retour sera le suivant :

# iptables -L

Chain INPUT (policy ACCEPT)

target prot opt source destination

Chain FORWARD (policy ACCEPT)

target prot opt source destination

Chain OUTPUT (policy ACCEPT)

target prot opt source destination

Vous pouvez vérifier que le firewall est actif avec la commande suivante :

# systemctl is-active iptables.service

active

Vous pouvez vérifier que le firewall est actif à chaque démarrage avec la commande suivante :

# systemctl is-enabled iptables.service

enabled

### Démarrage du service

La commande permettant de démarrer le pare-feu :

# systemctl start iptables.service

La commande permettant de démarrer le pare-feu automatiquement à chaque démarrage :

# systemctl enable iptables.service

### Arrêt du service

Il est déconseillé d’arrêter le pare-feu. Néanmoins, il peut être nécessaire de l’arrêter à des fins de diagnostique notamment :

# systemctl stop iptables.service

### Relance du service

La commande permettant de redémarrer le pare-feu :

# systemctl restart iptables.service

### Désactivation du Pare-Feu (uniquement sur une souche N1)

Sur la souche N1, il peut être décidé de désactiver le Pare-Feu.

La commande ci-dessous désactive le firewall au démarrage du système.

# systemctl disable iptables.service

rm '/etc/systemd/system/basic.target.wants/iptables.service'

La vérification de la prise en compte se fait avec la commande suivante :

# systemctl is-enabled iptables.service

disabled

### Ajout d’une règle

L’ajout d’une règle dans la configuration du pare-feu est sensible. Il est nécessaire d’ajouter une règle uniquement dans le cas d’un trafic entrant sur le serveur. Pour qu’une nouvelle règle (entrante) soit prise en compte, il est obligatoire qu’elle figure avant la ligne suivante dans la configuration du pare-feu :

REJECT all -- anywhere anywhere reject-with icmp-host-prohibited

Il est possible d’ajouter des règles de plusieurs façons. Cependant, une seule manière sera détaillée ici. La syntaxe de la commande recommandée est la suivante :

# iptables -I INPUT <NUM> -p <PROTO> --dport <PORT> -j ACCEPT -m comment --comment "<COMMENTAIRES>"

* **-I** permet d’insérer une règle
* **INPUT** ce sera une règle entrante
* **<NUM>** le n° que la règle aura dans la configuration
* **-p <PROTO>** le protocole réseau du flux entrant
* **--dport** indique le sens du flux (Destination Port = Port Local)
* **<PORT>** peut être un numéro de port, une liste (PORT1,PORT2,etc…) ou une plage (PORT\_DEBUT **:**PORT\_FIN)
* **-j ACCEPT**
* **-m comment --comment "<COMMENTAIRES>"** facultatif mais permet de mettre un commentaire pour la règle

Un exemple de commande est détaillé ci-dessous :

# iptables -I INPUT 6 -p tcp --dport 80 -j ACCEPT -m comment --comment "Serveur Web Local"

La commande ci-dessus permettra un accès au port TCP 80 local du serveur (port par défaut pour un serveur Web) depuis l’extérieur.

Exemple de sortie après l’ajout d’une règle :

# iptables -L

Chain INPUT (policy ACCEPT)

target prot opt source destination

ACCEPT all -- anywhere anywhere state RELATED,ESTABLISHED

ACCEPT icmp -- anywhere anywhere

ACCEPT all -- anywhere anywhere

ACCEPT tcp -- anywhere anywhere state NEW tcp dpt:ssh

ACCEPT tcp -- anywhere anywhere state NEW tcp dpt:51234

ACCEPT tcp -- anywhere anywhere tcp dpt:http /\* Serveur Web Local \*/

ACCEPT udp -- anywhere anywhere state NEW udp dpt:ntp

ACCEPT tcp -- anywhere anywhere state NEW tcp dpt:ntp

REJECT all -- anywhere anywhere reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)

target prot opt source destination

REJECT all -- anywhere anywhere reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)

target prot opt source destination

|  |  |
| --- | --- |
|  | Il est nécessaire de sauvegarder la configuration pour que les changements soient pris en compte après un redémarrage. |

### Sauvegarde de la configuration du pare-feu

Il est nécessaire de sauvegarder la configuration après chaque modification des règles du pare-feu. Les règles sont sauvegardées dans le fichier */etc/sysconfig/iptables*. Ce fichier sera lu à chaque démarrage du pare-feu.

La commande permettant d’effectuer la sauvegarde est la suivante :

# service iptables save

iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]

### Retrait d’une règle

Il peut être nécessaire de supprimer une règle de la configuration du pare-feu (exemple : suppression d’un OI).

La syntaxe de la commande de suppression est la suivante :

# iptables -D INPUT <NUM>

Où <NUM> correspond au numéro de règle à supprimer.

Exemple : En reprenant le chapitre **2.4.6**, pour supprimer la règle ajoutée, il faudrait passer la commande :

# iptables -D INPUT 6

On constate bien que la règle n°6 (ci-dessous) n’est plus présente dans la configuration :

ACCEPT tcp -- anywhere anywhere tcp dpt:http /\* Serveur Web Local \*/

# iptables -L

Chain INPUT (policy ACCEPT)

target prot opt source destination

ACCEPT all -- anywhere anywhere state RELATED,ESTABLISHED

ACCEPT icmp -- anywhere anywhere

ACCEPT all -- anywhere anywhere

ACCEPT tcp -- anywhere anywhere state NEW tcp dpt:ssh

ACCEPT tcp -- anywhere anywhere state NEW tcp dpt:51234

ACCEPT udp -- anywhere anywhere state NEW udp dpt:ntp

ACCEPT tcp -- anywhere anywhere state NEW tcp dpt:ntp

REJECT all -- anywhere anywhere reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)

target prot opt source destination

REJECT all -- anywhere anywhere reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)

target prot opt source destination

|  |  |
| --- | --- |
|  | Il est nécessaire de sauvegarder la configuration pour que les changements soient pris en compte après un redémarrage. |

# Multi-attachement réseau

## Redondance avec tolérance de panne simple

### Principe

Cette solution propose de configurer le multi-attachement réseau en mode actif/passif de manière à garantir une haute disponibilité de la connexion réseau. Si l’interface principale n’assure plus la liaison, la seconde interface prend le relais automatiquement au bout d’un court délai paramétrable.

L’objectif est d’utiliser les fonctionnalités de tolérance de panne du multi-attachement réseau, pour assurer la redondance de la connexion réseau. En cas de défaillance d’une interface (chemin réseau), l’interface de secours prend le relais sans perte de transactions.

La bascule du multi-attachement réseau de l’interface active défaillante vers la première interface passive en secours se fait sur un changement d’état de l’indicateur LINK DETECTED de l’interface qui était active.

Ce basculement se fait au bout d’un délai en millisecondes paramétré dans le lancement du module bonding.

Une fois que le basculement de continuité a eu lieu sur l’interface survivante, il n’y a pas de retour automatique sur le port d’origine même en cas de restauration de la liaison.

Si la nouvelle interface rencontre un souci, la bascule vers l’interface d’origine se fera automatiquement de la même façon si celle-ci a été remise en service entre temps.

### Pré-requis

Deux interfaces réseaux sont nécessaires sur la machine pour gérer le double attachement réseau en tolérance de panne. Ces deux interfaces doivent être sur deux cartes réseaux distinctes et branchées sur un commutateur différent.

### Opérations à effectuer

#### Module noyau bonding

Le module noyau bonding doit être préalablement chargé par la commande suivante :

# modprobe --first-time bonding

Pour que le module bonding soit chargé automatiquement à chaque démarrage de la machine il faut exécuter la commande suivante :

# echo "bonding" > /etc/modules-load.d/bonding.conf

#### Fichier /etc/sysconfig/network-scripts/ifcfg-<interface>

La mise en place du multi-attachement repose sur la création d’une interface réseau virtuelle qui se nommera « bondX » avec X commençant à 0 (zéro) pour le premier « channel bonding » demandé.

On doit donc créer un fichier /etc/sysconfig/network-scripts/ifcfg-bond0 de configuration d’une structure voisine de ceux des interfaces physiques présentes dans la machine, puis modifier les fichiers de configuration des interfaces physiques pour les intégrer dans le « channel bonding » souhaité.

Le nouveau fichier /etc/sysconfig/network-scripts/ifcfg-bond0 doit contenir :

DEVICE=bond0

NAME=bond0

TYPE=Bond

BONDING\_MASTER=yes

IPADDR=<ADRESSE IP DE LA MACHINE>

PREFIX=<MASQUE IP DE LA MACHINE au format /XX>

GATEWAY=<Adresse IP de la passerelle par defaut>

ONBOOT=yes

BOOTPROTO=none

BONDING\_OPTS="mode=1 miimon=100"

Le paramètre « miimon » passé au pilote indique le délai de perte de lien en millisecondes au bout duquel le basculement sur la prochaine carte survivante doit avoir lieu.

Le paramètre « mode » passé au pilote indique qu’on demande un fonctionnement en tolérance de panne.

La ligne GATEWAY peut ne pas être renseignée si la passerelle par défaut est renseignée dans le fichier /etc/sysconfig/network

Le fichier /etc/sysconfig/network-scripts/ifcfg-en\*X de configuration de la première interface physique doit contenir (dans notre exemple la première interface est ens32):

DEVICE= ens32

NAME=bond0-slave

TYPE=Ethernet

UUID="<UUID DE L’INTERFACE>"

BOOTPROTO=none

ONBOOT=yes

MASTER=bond0

SLAVE=yes

Le fichier /etc/sysconfig/network-scripts/ifcfg-en\*Y de configuration de la seconde interface physique doit contenir (dans notre exemple la seconde interface est ens34) :

DEVICE=ens34

NAME=bond0-slave

TYPE=Ethernet

UUID="<UUID DE L’INTERFACE>"

BOOTPROTO=none

ONBOOT=yes

MASTER=bond0

SLAVE=yes

Les deux fichiers ifcfg-ens32 et ifcfg-ens34 ne comportent plus de configuration TCP/IP. Ils font tous les deux références à l’interface bond0.

L’UUID de l’interface et doit être différente dans chacun d’entre eux.

|  |  |
| --- | --- |
|  | SRT ne garantit pas l’auto-négociation de ses commutateurs, ainsi à partir de la publication 5.4 du palier système RHEL 5 le 100baseT/Full duplex est forcé. Pour débrider l’interface réseau, veuillez vous référer à la procédure technique d’exploitation du palier système. |

#### Réactivation des interfaces réseau et redémarrage du service réseau

|  |  |
| --- | --- |
|  | Si vous accédez à la machine via le réseau, la désactivation d’une interface ou l’arrêt-relance du service réseau coupera votre session, et toute erreur de configuration imposera un accès local pour corriger. |

On demande la réactivation de la première interface réseau :

# ifdown ens32 ; ifup ens32

On demande la réactivation de la seconde interface réseau :

# ifdown ens34 ; ifup ens34

On demande la réactivation de l’interface de bonding :

# ifdown bond0 ; ifup bond0

|  |  |
| --- | --- |
|  |  |

On demande l’arrêt-relance du service réseau :

# systemctl restart network

### Vérification de la mise en place

La vérification de la prise en compte du multi-attachement se fait par l’affichage des informations d’interfaces réseaux avec la commande ip link. Le résultat montre les interfaces physiques ainsi que l’interface de multi-attachement (exemple de machine représentative) :

# ip link

1: lo: <LOOPBACK,UP,LOWER\_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT

link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00

2: ens32: <BROADCAST,MULTICAST,SLAVE,UP,LOWER\_UP> mtu 1500 qdisc pfifo\_fast master bond0 state UP mode DEFAULT qlen 1000

link/ether 00:50:56:a4:00:6e brd ff:ff:ff:ff:ff:ff

4: ens34: <BROADCAST,MULTICAST,SLAVE,UP,LOWER\_UP> mtu 1500 qdisc pfifo\_fast master bond0 state UP mode DEFAULT qlen 1000

link/ether 00:50:56:a4:00:6e brd ff:ff:ff:ff:ff:ff

5: bond0: <BROADCAST,MULTICAST,MASTER,UP,LOWER\_UP> mtu 1500 qdisc noqueue state UP mode DEFAULT

link/ether 00:50:56:a4:00:6e brd ff:ff:ff:ff:ff:ff

On remarque que toutes les interfaces physiques ou virtuelles impliquées dans la création d’un même agrégat portent à la fois la même adresse IP et la même adresse MAC, ce n’est pas une anomalie, c’est le principe même du bonding.

|  |  |
| --- | --- |
|  | Le mode « 1 » est un mode actif-passif qui laisse l’interface passive déconnectée (« down ») tant qu’elle n’est pas utilisée, si bien qu’aucune perturbation n’est possible par duplication d’une adresse MAC. |

On peut également consulter l’état du multi-attachement en temps réel :

# cat /proc/net/bonding/bond0

Ethernet Channel Bonding Driver: v3.7.1 (April 27, 2011)

Bonding Mode: fault-tolerance (active-backup)

Primary Slave: None

Currently Active Slave: ens32

MII Status: up

MII Polling Interval (ms): 100

Up Delay (ms): 0

Down Delay (ms): 0

Slave Interface: ens32

MII Status: up

Speed: 1000 Mbps

Duplex: full

Link Failure Count: 0

Permanent HW addr: 00:50:56:a4:00:6e

Slave queue ID: 0

Slave Interface: ens34

MII Status: up

Speed: 1000 Mbps

Duplex: full

Link Failure Count: 0

Permanent HW addr: 00:50:56:b1:b1:3a

Slave queue ID: 0

Si le lien avec ens32 est perdu on constate le basculement sur ens34 :

# cat /proc/net/bonding/bond0

Ethernet Channel Bonding Driver: v3.7.1 (April 27, 2011)

Bonding Mode: fault-tolerance (active-backup)

Primary Slave: None

Currently Active Slave: ens34

MII Status: up

MII Polling Interval (ms): 100

Up Delay (ms): 0

Down Delay (ms): 0

Slave Interface: ens34

MII Status: up

Speed: 1000 Mbps

Duplex: full

Link Failure Count: 0

Permanent HW addr: 00:50:56:b1:b1:3a

Slave queue ID: 0

Le basculement est également observé dans /var/log/messages :

kernel: bonding: bond0: releasing active interface ens32

kernel: bonding: bond0: making interface ens34 the new active one.

Il est conseillé d’effectuer un redémarrage du serveur pour valider l’ensemble des configurations réseaux et modules noyaux après la mise en place du multi-attachement. L’analyse de /var/log/messages est également conseillée une fois le redémarrage effectué.

La commande ifenslave permet de manipuler le bonding (bascule de cartes, etc…)

Exemple pour changer l’interface active (si ens32 redevient opérationnelle) :

# ifenslave -c bond0 ens32

# cat /proc/net/bonding/bond0 | grep "Active Slave"

Currently Active Slave: ens32

ens32 est maintenant l’interface active.

|  |  |
| --- | --- |
|  | Le fonctionnement est symétrique sur les deux interfaces, forcer le basculement vers une interface spécifique n’est donc pas nécessaire. |

# Bibliographie

* <https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux>
* <https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html-single/Networking_Guide/index.html>
* <https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html-single/Networking_Guide/index.html#sec-Using_Channel_Bonding>
* **https://access.redhat.com/documentation/en-US/Red\_Hat\_Enterprise\_Linux/7/html-single/Networking\_Guide/index.html#ch-Configure\_Network\_Teaming**
* <http://kbase.redhat.com/faq/docs/DOC-15331>
* http://kbase.redhat.com/faq/FAQ\_79\_899.shtm
* <http://kbase.redhat.com/faq/docs/DOC-7431>
* <http://kbase.redhat.com/faq/docs/DOC-28122>
* <http://www.kernel.org/doc/Documentation/networking/bonding.txt>
* ✦ Fin du document ✦

1. Par exemple, par l’utilisateur root via un sudo, etc [↑](#footnote-ref-1)