Haute disponibilité d'un serveur FTP

Propriétés	Description
Type de publication	Côté Labo
Intitulé court	**Haute disponibilité d'un serveur FTP (File Transfert Protocol)**
Intitulé long	**Haute disponibilité d'un serveur FTP** avec synchronisation des données via DRBD
Module	BTS SIO2 – **SISR3 – Exploitation des services**
Date de publication	Septembre 2013
Date de modification	Octobre 2016
Version	V2.0
Présentation	L'objectif de ce Côté Labo (mis en œuvre en module) est de poursuivre la mise en haute disponibilité des services (Coté Labo « Haute disponibilité du service Web ») en intégrant le serveur FTP. Il est décomposé en 2 activités : Activité 1 : installation et configuration de DRBD Activité 2 : intégration de la solution au cluster
Activités	**D1.3 - Mise en production d'un service** • A1.3.2 Définition des éléments nécessaires à la continuité d'un service **D2.1 - Exploitation des services** • A2.1.2 Évaluation et maintien de la qualité de service **D3.2 - Installation d'une solution d'infrastructure** **D3.3 - Administration et supervision d'une infrastructure** • A3.3.1 Administration sur site ou à distance des éléments d'un réseau, de serveurs, de services et d'équipements terminaux
Pré-requis	Avoir quelques notions sur l'installation, la configuration et l'administration d'un serveur Linux. Avoir réalisé le Coté Labo « Haute disponibilité du service Web » (http://www.reseaucerta.org/hd-service-web-dynamique). Connaître le rôle et les principaux concepts du service FTP. Connaître le rôle et les principaux concepts d'un système de gestion de fichiers.
Savoir-faire principaux	**En SISR3** : • Caractériser les éléments nécessaires à la qualité, à la continuité et à la sécurité d'un service • Installer et configurer les éléments nécessaires à la qualité et à la continuité du service • Valider et documenter la qualité, la continuité et la sécurité d'un service

Transversalité	**SI7** : • Justifier le choix d'une solution de mise en production d'un service • Stratégies et techniques associées à la continuité de service • Stratégies et techniques de sauvegarde et de restauration de données • Stratégies et techniques de répartition et de réplication **SISR4** : • Justifier le choix d'une solution de gestion de la disponibilité d'un serveur • Installer et configurer une solution de disponibilité de serveurs • Disponibilité des systèmes, méthodes, technologies, techniques, normes et standards associés **En SISR5** : • Assurer la haute disponibilité des services réseau (DNS, DHCP, etc) • Assurer la haute disponibilité du matériel d'interconnexion • Superviser le cluster
Prolongements	**En SI7** : • Rédiger, mettre en place et tester un Plan de Continuité d'Activité (PCA) **En SISR3** : • Affiner la configuration de DRBD • Assurer la haute disponibilité d'autres services aux utilisateurs • Intégrer un autre nœud dans le cluster • Intégrer la répartition de charges • Authentification LDAP pour le service FTP
Outils	**SE** : Serveur Linux Debian Jessie (stable actuelle) **Serveurs/services** : proftpd installé et configuré à l'identique sur les deux serveurs, Corosync et Pacemaker. **Clients** : client FTP sur STA Linux, Windows ou autre système. **Contexte** : organisation/GSB-Organisation.doc. **Documentation** : organisation/outils/GSB-DocumentTechnique.doc **Site officiel de Pacemaker** : http://clusterlabs.org/ **Documentation** : http://clusterlabs.org/doc/en-US/Pacemaker/1.1/html/Clusters_from_Scratch/ **Site officiel de DRBD :** /www.drbd.org/ et plus particulièrement http://www.drbd.org/en/doc/users-guide-84
Mots-clés	Disponibilité, HA, HD, Corosync, Pacemaker, synchronisation, FTP, DRBD
Durée	8 heures
Auteur(es)	Apollonie Raffalli avec la relecture attentive de Rogez Sanchez et Gaëlle Castel et celle de Yann Barrot pour cette deuxième version.

La haute-disponibilité d'un serveur de fichiers

Dans le précédent Côté Labo, nous avons installé une solution de haute disponibilité du service Web pour l'application *de gestion de frais* avec retour automatique vers le serveur primaire.

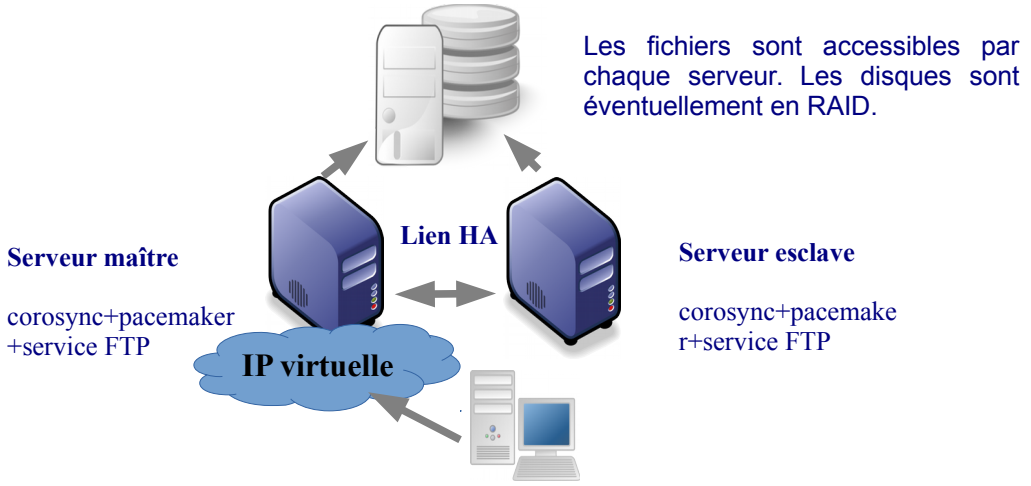
Nous proposons ici de compléter les services aux utilisateurs mis en haute disponibilité avec un serveur FTP qui mettra à disposition (en lecture et écriture) certains répertoires du disque.

En mettant en œuvre les mêmes technologies, nous aurions aussi pu compléter la HD du service Web en assurant la synchronisation de l'espace de stockage des pages Web statiques mais le choix de visiter une autre service a été fait.

Comme pour un serveur Web dynamique, la haute disponibilité d'un serveur de fichier nécessite une solution qui va permettre de répliquer les données de manière à ce que si le serveur de secours venait à prendre le relais, il dispose des données actuelles. De même pour le retour vers le serveur d'origine.

Plusieurs architectures sont possibles.

Les données sont stockées sur un serveur « à part » (un serveur NAS par exemple) :

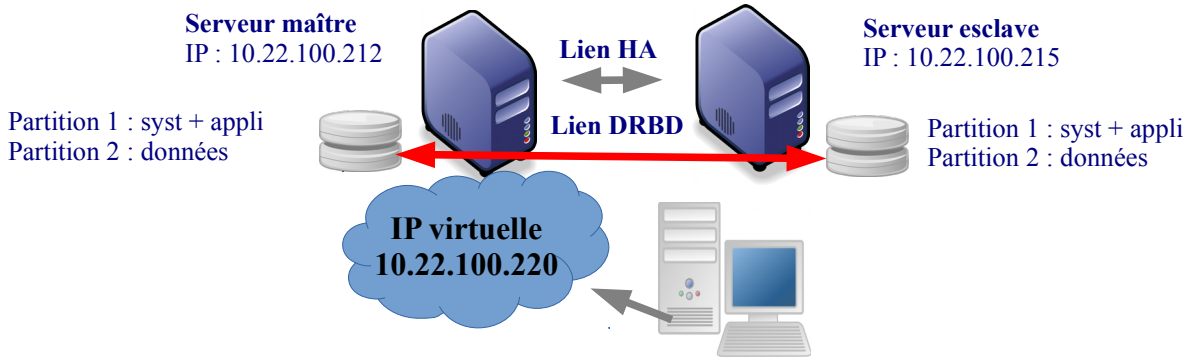


Tout ce qui est écrit sera retrouvé par l'autre machine, mais nous introduisons ici un point de faiblesse car en cas de défaillance du serveur de fichiers lui-même (et pas seulement d'un disque), les données ne sont plus disponibles.

Il faut donc assurer aussi la haute disponibilité du serveur de fichier en synchronisant en temps réel les fichiers sur une autre machine. La solution la plus simple pour créer ce type de serveur est d'utiliser **DRBD (Distributed Replicated Block Device** en anglais, ou périphérique en mode bloc répliqué et distribué)C'est un outil qui synchronise (par réplication) des périphériques de stockage (partition, volume logique, etc.) entre deux nœuds via le réseau (une sorte de RAID 1 réseau).

Pour utiliser DRBD et synchroniser des données, il n'est pas nécessaire d'utiliser un serveur « à part », il suffit d'isoler les données à synchroniser sur une partition ou un volume logique : **c'est l'architecture que nous allons utiliser.**

Les données sont stockées dans une partition sur chaque serveur :



Contexte

Le laboratoire pharmaceutique Galaxy-Swiss Bourdin (GSB) met à disposition des visiteurs médicaux une application Web sécurisée de gestion des frais de remboursement (Côté Labo « Service Web sécurisé »). La haute disponibilité de cette application est assurée via un serveur de secours (Côté Labo « haute disponibilité du service Web »).

GSB dispose ainsi :

- d'un serveur maître *intralabXX* ;
- d'un serveur de secours *hdintralabXX*.

où XX représente les initiales de vos prénoms et noms.

La mise en œuvre de la haute disponibilité a été simulée sur des machines virtuelles présentes dans la ferme des serveurs et le cluster est accessible par son adresse IP virtuelle correspondant au nom DNS « servIntralabXX.gsb.coop ».

Il a été décidé de mettre à disposition sur le serveur *intralabXX* un service FTP (le paquetage *proftpd*) utile aux développeurs de GSB pour transférer leurs fichiers. Ce service sera intégré à la solution de haute disponibilité.

Les exemples de configuration sont basés sur la configuration suivante (à adapter) :

intralabXX : serveur maître

- IP réelle : 10.22.100.212 --> c'est celle qui est dans /etc/network/interfaces
- IP virtuelle : **10.22.100.220**

hdintralabXX : serveur esclave

- IP réelle : 10.22.100.215 --> c'est celle qui est dans /etc/network/interfaces
- IP virtuelle **: 10.22.100.220**

Le Coté Labo est composé de 2 activités.

L'activité 1 consiste à préparer les serveurs et à installer et configurer DRBD.
L'activité 2 consiste à intégrer la solution au cluster de manière à ce qu'en cas d'un serveur défaillant, la bascule vers l'autre serveur soit automatisée.