Spécification de l'architecture DNS

H4413

11 mai 2011

Table des matières

1 Proposition d'une architecture adaptée

1.1 Architecture multi-sites du service d'annuaire

Répartition de l'annuaire LDAP sur plusieurs machines. On utilise la méthode de réplication, on aura donc sur chaque site géographique une machine contenant une copie de l'annuaire. Cela permet de toujours se connecter au serveur le plus proche de l'utilisateur envoyant une requête et en plus une résistance aux pannes. En effet, si le serveur du site géographique est en panne, on peut se connecter à un des autres serveurs sur site distant.

1.2 Architecture DNS

On mettra en place un serveur DNS par site où se trouve l'AIP. Ceux-ci géreront les accès extérieurs au réseau au niveau de la connexion vers l'établissement. De plus ils connaîtront les autres serveurs DNS des sites distants de l'AIP.

On veillera à ajouter les entrées de type (R) concernant les serveurs DNS de l'AIP sur les serveurs de niveaux supérieurs possédés par les établissements.

1.3 Politique de nommage

De manière générale, l'ensemble de numérotation comprenant des "xx", signifient que la numérotation peut aller de 01 à 99.

1.3.1 Niveau Site

Le nom du site sera choisi pour AIPRAO. La seconde extension sera choisie en fonction du site ou se trouve l'objet réseau concerné.

Exemple : ge.aiprao pour les objets du bâtiment du site GE.

Nous choisissons pour l'ensemble des sites :

- central.aiprao
- ge.aiprao
- roanne.aiprao

1.3.2 Serveurs

Nous créons un sous domaine appelé serveur. Les serveurs auront pour nom leur principale fonctionnalité associée à leur numéro de serveur.

Exemple : Nom du serveur LDAP situé au bâtiment central : ldap-01.serveur.central.aiprao

1.3.3 Niveau Salle

Les PC auront pour nom "pc-xx", xx étant le numéro du pc. Le premier PC aura pour numéro 01.

Exemple : le situé pc en GE aura pour nom pc-01.ge.aiprao .

1.3.4 Site Central

Les plateformes de manipulation auront pour nom de domaine "pl-xx".

Les automates auront pour nommage "a-xx".

Exemple : le deuxième automate de la première plateforme aura pour nom :
a-02.pl-01.central.aiprao

Les webcams auront pour nom "webcam-xx".

1.4 Relation entre les serveurs

Les différents serveurs communiquent entre eux en fonction du nom de domaine. Le DNS local permet d'identifier directement une machine sur son réseau local.

1.5 Enregistrements

A nom d'hôte correspondant à une adresse IPv4 ;
[name] IN A [IPv4] aiprao.insa-lyon.fr IN A 10.0.0.11

AAAA nom d'hôte correspond à une adresse IPv6 ;
[name] [number] IN AAAA [IPv6] www.l.google.com. 77 IN AAAA 2a00 :1450 :8004 : :68

CNAME record ou canonical name record qui permet de créer un alias entre 2 domaines ;
[name] IN CNAME [name] aiprao.insa-lyon.fr. IN CNAME central.aiprao.insa-lyon.fr.

PTR record ou pointer record qui associe une adresse IP à un enregistrement de nom de domaine, aussi dit « reverse », il est le complémentaire de l'enregistrement A ;
[IP] IN PTR [name] 10.0.0.11 IN PTR aiprao.insa-lyon.fr.

NS record ou name server record qui définit les serveurs DNS de ce domaine ;
[name] NS [name] aiprao.insa-lyon.fr NS dns.aiprao.insa-lyon.fr.

SOA record ou Start Of Authority record qui donne les informations générales de la zone : serveur principal, courriel de contact, différentes durées dont celle d'expiration, numéro de série de la zone ; [name] IN SOA [name] [email] [serial] [refresh] [retry] [expire] [minimumTTL] aiprao.insa-lyon.fr IN SOA dns.aiprao.insa-lyon.fr. admin.aiprao.insa-lyon.fr. 2010060311 43200 7200 1209600 3600

2 Mise en place de procédures adaptées

Le serveur DHCP est utilisé pour pourvoir des adresses IP aux machines et accessoires branchés localement. En vue d'obtenir un adresse pour un nouveau dispositif, il suffit de la connecter physiquement à une prise RJ45. On veillera à configurer le DNS de manière manuel, méthode jugée la plus simple, car les machines seront "statiques".

Voici les étapes pour ajouter une machine :

Configuration du DNS , en ajoutant un enregistrement de type A ou AAAA sur le serveur DNS : le_nom_de_ma_nouvelle_machine IN A l_adresse_ip_de_ma_machine

Propogation des nouvelles informations , en modifiant l'enregistrement SOA du serveur DNS, associée au sérial vu dans la partie précédente. On y modifie les valeurs pour y mettre le jour d'aujourd'hui, sous la forme YYYYMMDD.

3 Configuration DHCP

'x' correspond au site de 1 à 4 : 1 pour Lyon, 2 pour la salle GE, 3 pour Roanne, 4 pour Saint-Etienne.

3.1 Adresse réseau

L'adresse du serveur DHCP sur chaque site sera 10.0.x.252.

3.2 Masque de sous réseau

255.255.255.0

3.3 Plage d'adresses IP de réseau

Les adresses IP des machines sont sur la plage 10.0.x.1 à 10.0.x.250. On peut donc connecter 250 machines par sous-réseau.

3.4 Durée du bail

La durée du bail sera fixée à long pour éviter les conflits si trop de machines viennent à être connectées.

3.5 Routeur

L'adresse du routeur sur chaque site sera de 10.0.x.254.

3.6 Adresse du DNS

L'adresse du serveur DNS sur chaque site sera 10.0.x.253.

3.7 Nom de l'étendue

On va faire 2 étendues par site : de 10.0.x.1 à 10.0.x.64 pour les automates et de 10.0.x.250 pour les autres machines.

3.8 Plage de l'exclusion

La plage de l'exclusion de chacune des 2 étendues est évidemment la plage de l'autre étendue.

3.9 Associations MAC/IP

Une adresse IP est attribuée à une adresse MAC tant qu'il reste des adresses disponibles pour les adresses MAC qui n'ont pas encore d'IP attribuée. Si les adresses sont toutes déjà attribuées sur un site et qu'une nouvelle machine se connecte, l'adresse IP qui n'a pas été utilisée depuis le plus de temps est réattribuée à cette nouvelle adresse MAC.