CRÉER UN SERVEUR MAIL SUR UN NAS SYNOLOGY

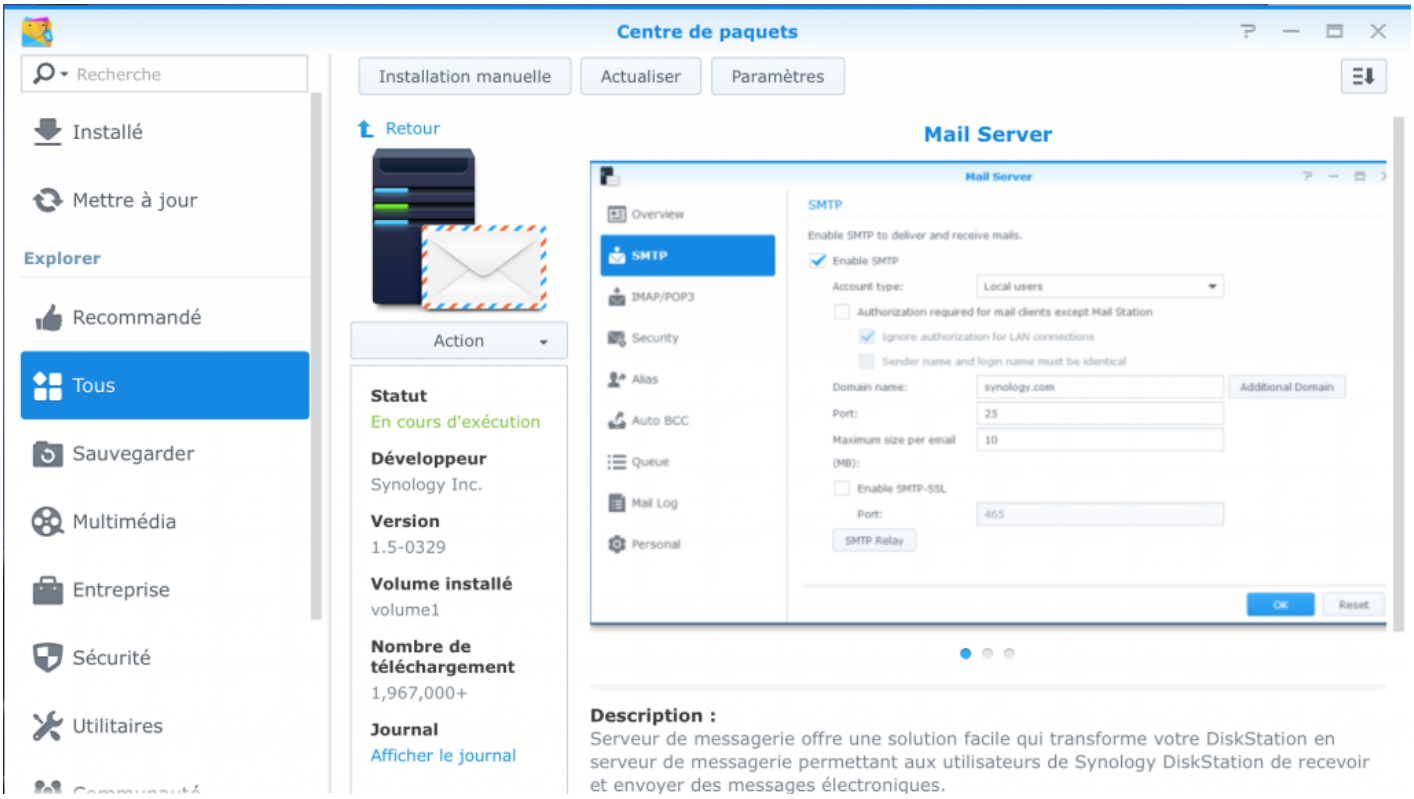
Synology propose de nombreux paquets à installer sur ses NAS pour lui ajouter des fonctionnalités. Parmi eux on trouve le paquet **Mail Server**.
Cette interface pour **Postfix** permet de mettre en place un véritable serveur mail, avec DKIM, DMARC etc… Il convient tout à fait pour un usage personnel ou pour une petite entreprise.
Nous allons donc voir comment configurer ce serveur et lui permettre d'envoyer des mails vers les grands fournisseurs type GMAIL et cie sans être déclaré en tant que SPAM.

PRÉ REQUIS

– Un NAS Synology
– Un nom de domaine et un accès à sa **zone DNS**
– Une adresse IP publique fixe est **indispensable** pour le serveur mail !!!

INSTALLATION DE MAIL SERVER

Nous allons installer le paquet proposé sur le store de **Synology**. Il nécessite l'installation du paquet **Perl** pour fonctionner.

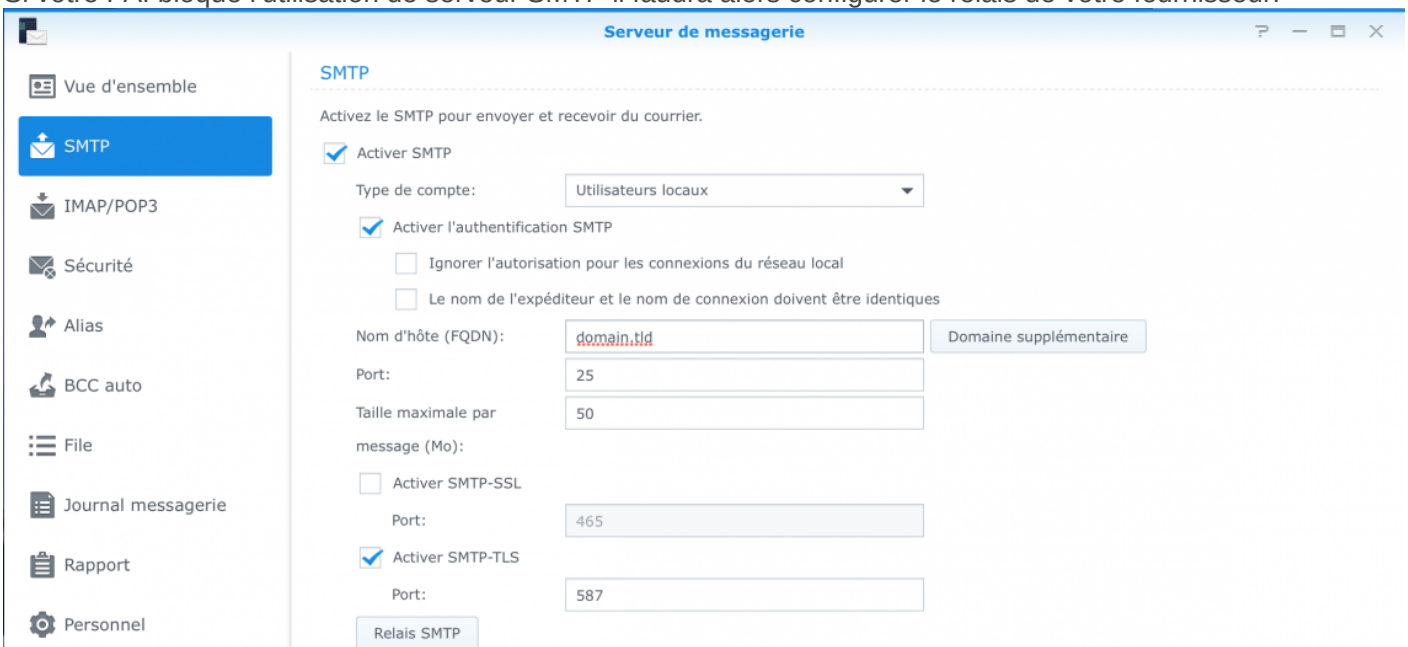


Si à la fin de l'installation le paquet ne s'est pas lancé, il est possible de le faire à l'aide du menu de gauche.

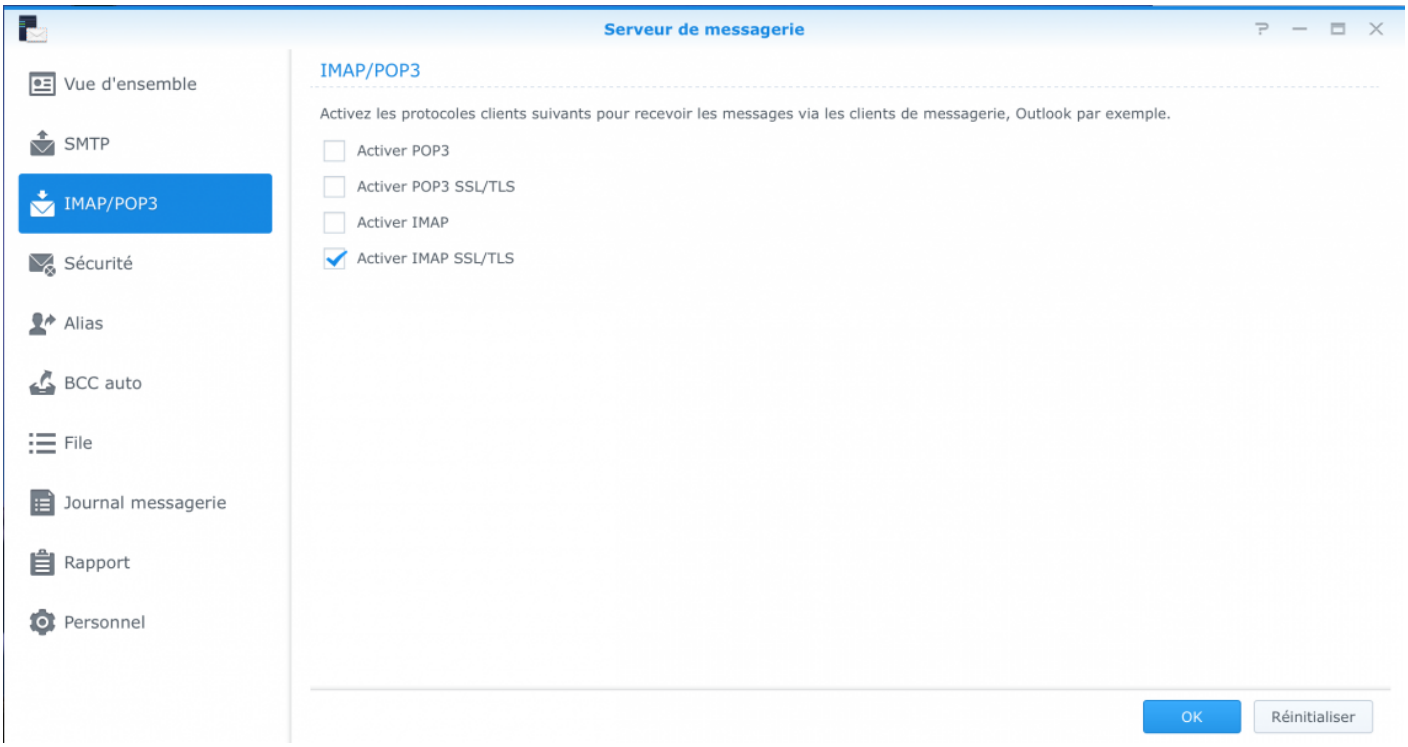
PARAMÈTRE IMAP / SMTP

Après l'installation on peut ouvrir l'interface d'administration de **Mail Server**.
Nous allons voir onglet par onglet les configurations à faire pour le rendre fonctionnel.

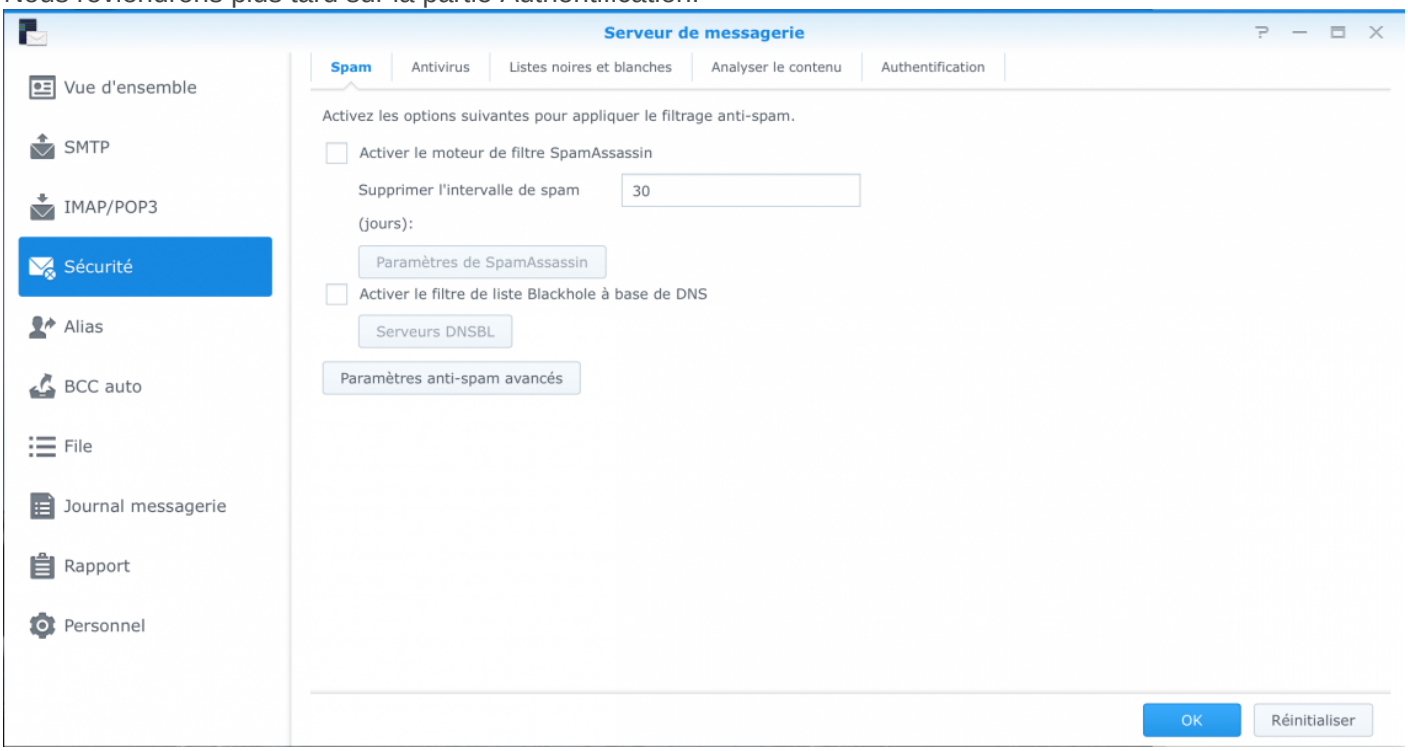
La **vue d'ensemble** n'est pas très importante, elle permet simplement d'avoir des statistiques sur le nombre de mails envoyés et reçus par le serveur, ainsi que sa consommation en bande passante.
Dans l'onglet **SMTP** nous allons configurer l'authentification sur notre serveur.
Dans un premier temps nous allons cocher « Activer SMTP ».
Pour le type d'utilisateur, vous aurez le choix d'utiliser les utilisateurs locaux sur votre NAS, ou d'utiliser les utilisateurs d'un annuaire Active Directory ou LDAP si votre NAS est associé à l'un d'entre eux.
Pour éviter que n'importe qui utilise notre serveur d'envoi nous activerons également l'authentification SMTP.
Dans le champ nom d'hôte, nous allons entrer le nom de domaine qui correspondra aux adresses mail. Ex : *domain.tld* enverra des mails en *someone@domain.tld*
Nous allons également activer le SMTP-TLS pour chiffrer les échanges avec notre serveur mail.
Si votre FAI bloque l'utilisation de serveur SMTP il faudra alors configurer le relais de votre fournisseur.



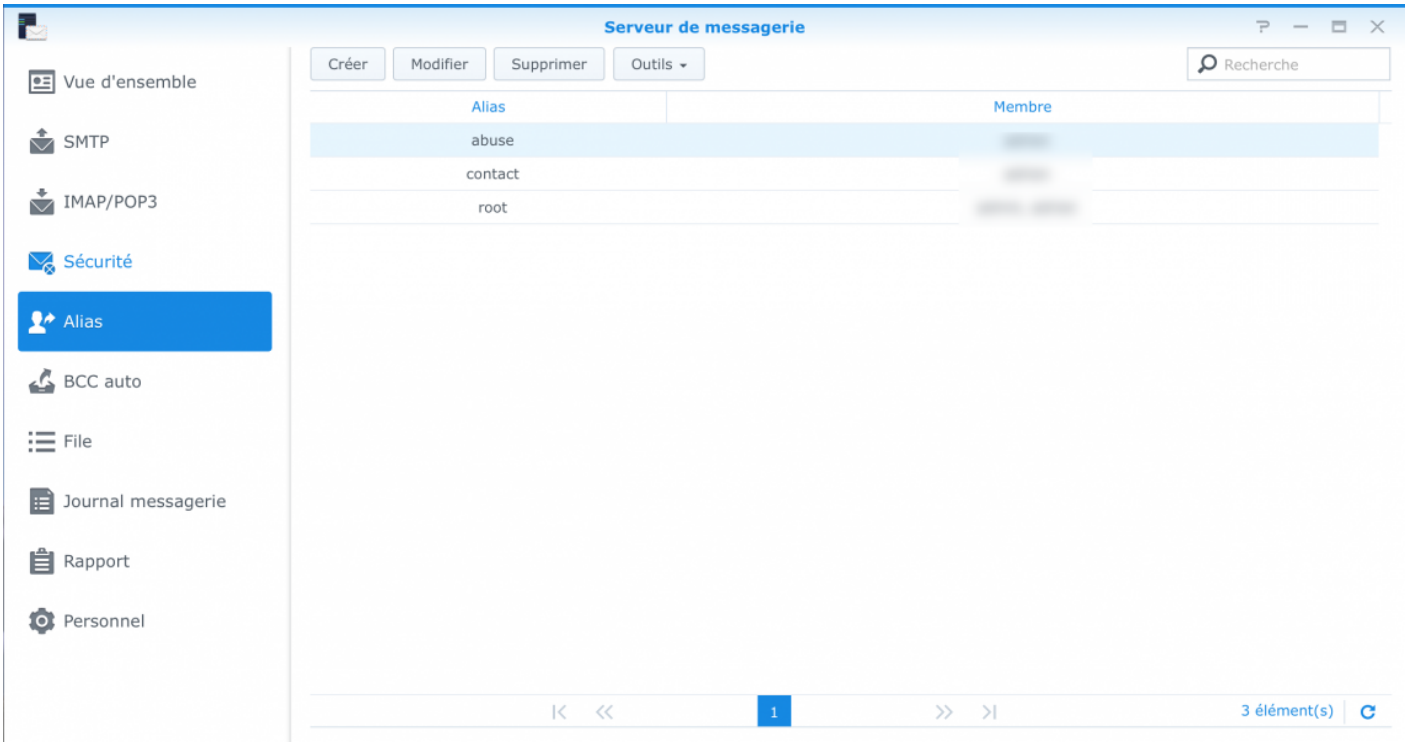
Dans l'onglet **IMAP/POP3** nous activerons uniquement l'IMAP SSL/TLS. Qui utilise encore du POP sérieusement ?



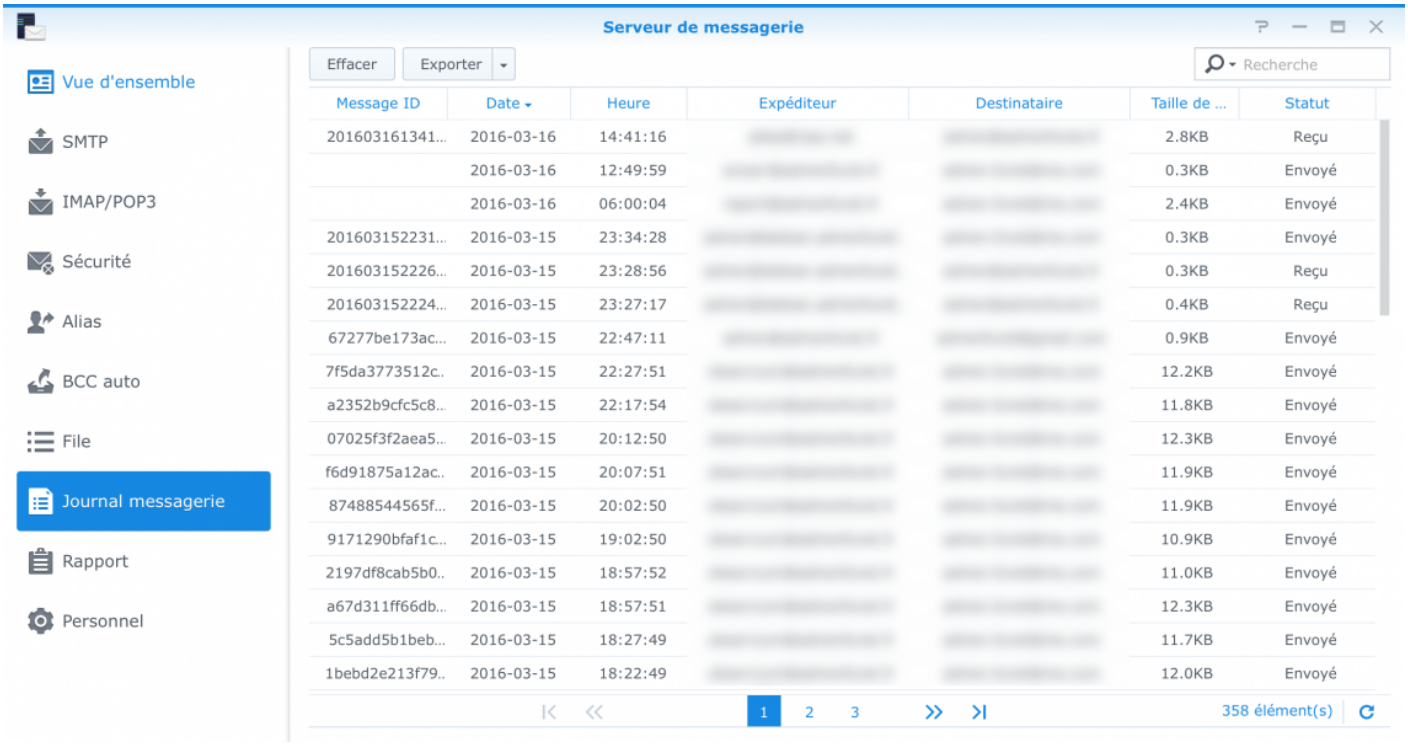
Dans l'onglet **Sécurité** il est possible de définir les règles d'analyses de SPAM Assassin et de l'antivirus. Dans un premier temps je vous déconseille de les activer immédiatement, et plutôt petit à petit pour avoir des réglages fins qui correspondent à votre besoin. En effet des réglages trop agressifs vous empêcheront peut-être d'envoyer ou recevoir des mails de certaines personnes.
Nous reviendrons plus tard sur la partie Authentification.



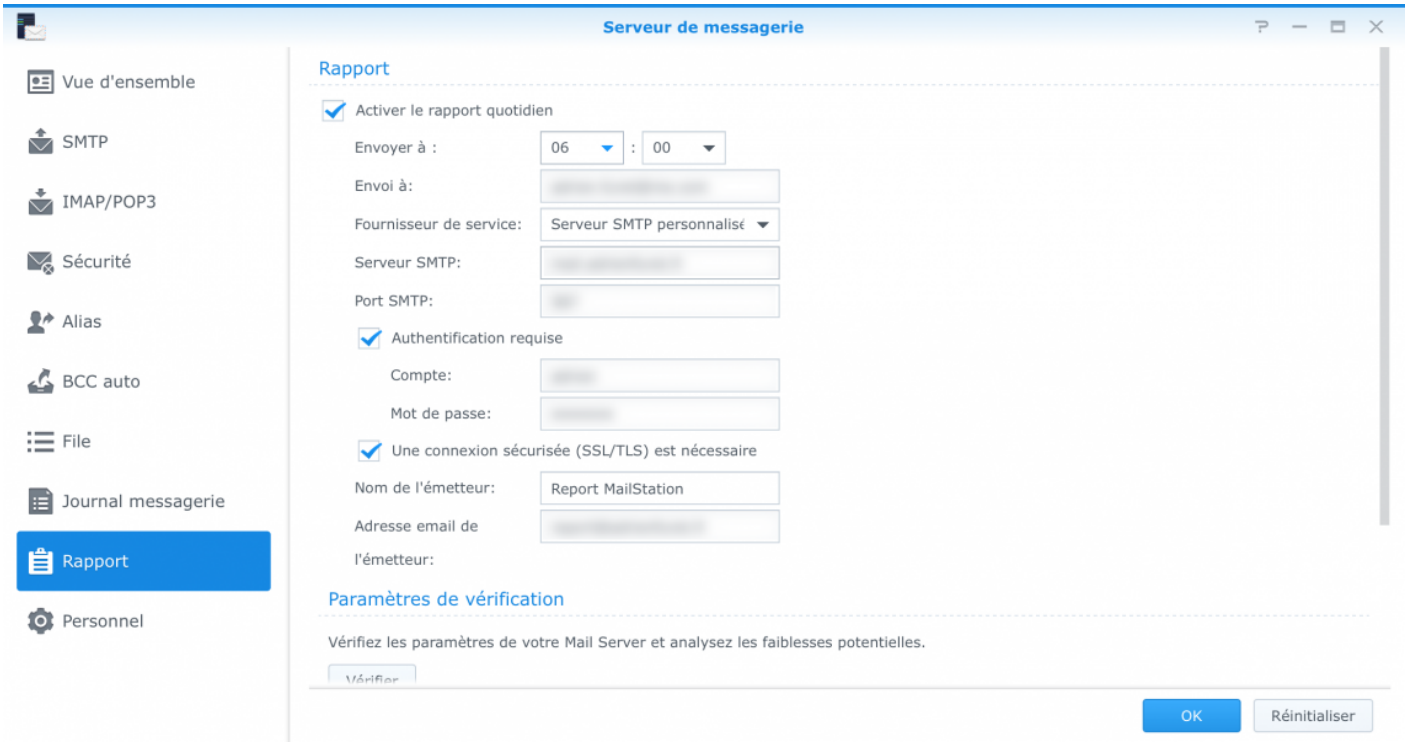
L'onglet **Alias** permet, comme son nom l'indique, de créer des alias ou listes de distribution. Pratique pour éviter d'avoir plusieurs boites pour une seule et même personne.
Il est également possible de renvoyer un alias sur une boîte aux lettre externe. Ce qui permet d'unifier les mails de contact si on a plusieurs domaines par exemples.
Je vous conseille de créer l'alias *abuse*, utilisés par les fournisseurs de mails pour vous envoyer des rapports.



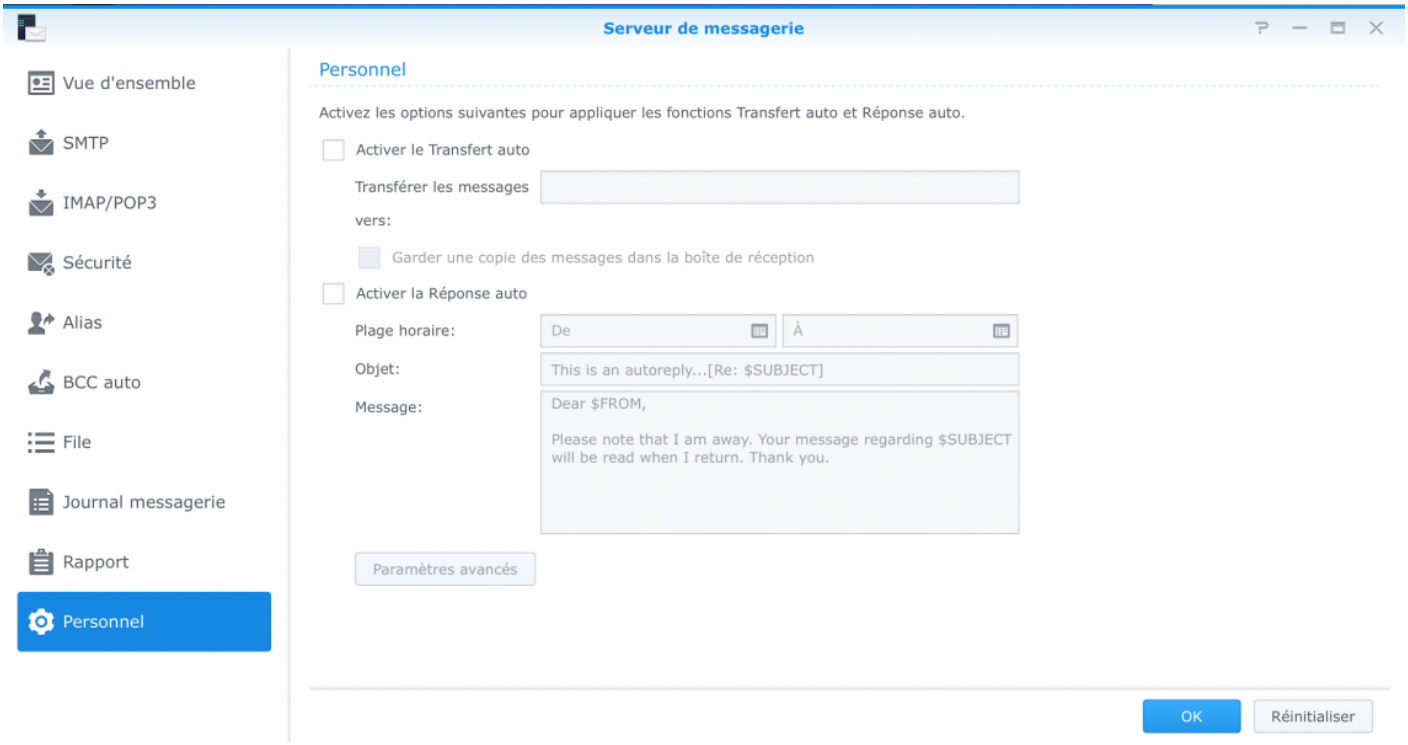
L'onglet **BCC** permet de définir des règles pour recevoir une copie des mails entrants/sortants selon certains critères. Personnellement je ne m'en sers pas.
Le **journal de messagerie** permet d'obtenir une liste de tous les mails passants par votre serveur.



Dans **Rapport** il est possible de régler l'envoi des statistiques du serveur à l'administrateur.



Pour terminer, l'onglet **personnel** permet de définir des réponses automatiques ou de transfert des mails.



PARAMÈTRES DE LA ZONE DNS

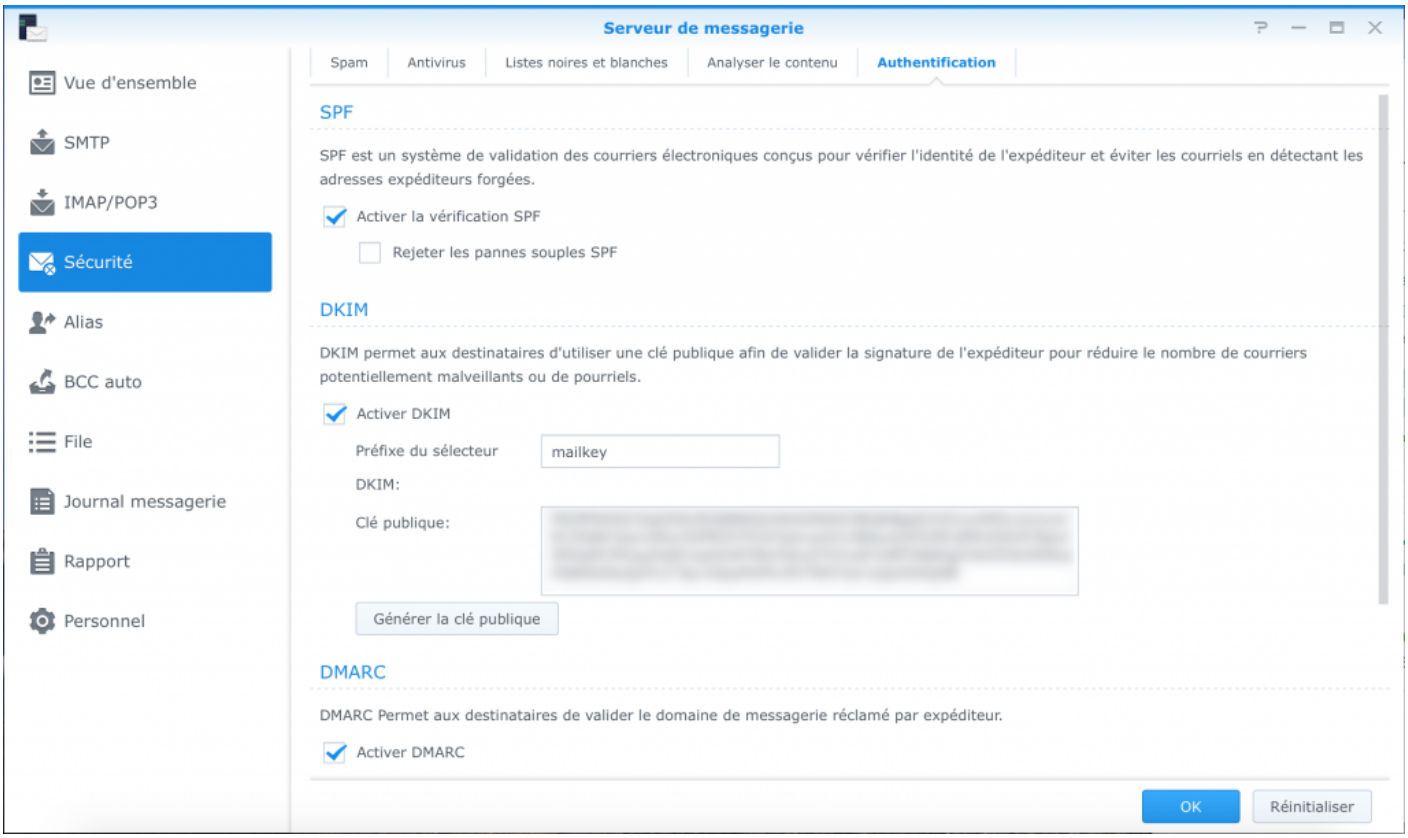
Nous allons désormais créer un **enregistrement DNS** pour notre serveur mail.

L'interface ci dessous est celle d'OVH, mais le principe reste le même pour les autres fournisseurs de domaine.
Nous allons créer un enregistrement de **type A** pour le sous domaine *mail.domain.tld* pointant sur l'**IP publique** de notre serveur mail.

Puis nous allons ajouter un enregistrement **MX** pour notre domaine pointant sur le sous domaine *mail.domain.tld*, avec une priorité de **10**.

AJOUT DE SPF, DKIM, ET DMARC

Pour vérifier l'authenticité d'un mail et le classer en tant que SPAM ou non, les serveurs vérifient différents paramètres comme le **SPF**, le **DKIM** et le **DMARC** (pour en savoir plus sur ces trois enregistrement je vous invite à consulter la page Wikipédia correspondante).
Nous allons donc ajouter ces enregistrements pour éviter que tous nos mails sortants ne soient considérés en tant que SPAM.
Sur **Mail Server** nous allons donc retourner sur l'onglet **Sécurité -> Authentification**.
Nous allons cocher la vérification **SPF**.
Nous allons activer le **DKIM**, en mettant le sélecteur suivant : *mailkey* et générant une **clé publique**.
Elle s'affichera dans le cadre en dessous, alors que notre clé privée sera stockée sur le NAS.
Puis nous activerons le **DMARC**.



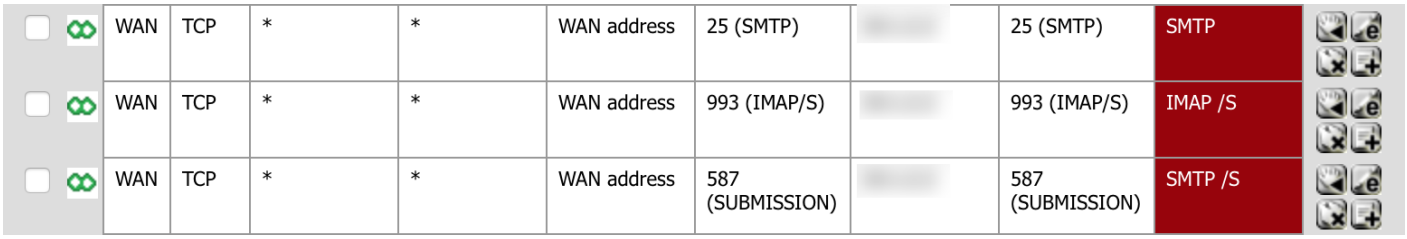
Il va maintenant falloir ajouter ces paramètres à notre zone DNS pour que les autres serveurs puissent les consulter.
Pour le **SPF** nous allons créer un enregistrement TXT avec notre domaine racine (*domain.tld*) et la valeur suivante : *v=spf1 a mx ip4:11.22.33.44 ~all*
En remplaçant 11.22.33.44 par l'IP publique de notre NAS.

Pour le **DKIM** nous allons également créer un enregistrement TXT avec le sous domaine *mailkey._domainkey.domain.tld* et la clé publique générée sur le NAS.
t=s; p=cle_publique
En remplaçant bien sur cle_publique par la clé générée par Mail Server.

Enfin pour le **DMARC** nous créerons un enregistrement TXT avec le sous domaine *_dmarc.domain.tld* et la valeur suivante :
v=DMARC1; p=none

Votre serveur mail est désormais correctement configuré.

Il reste désormais à ouvrir les ports de Firewall et les rediriger vers le NAS.
Il faut ouvrir les ports **25** et **587** pour le SMTP et le port **993** pour l'IMAP SSL/TLS.



☐	WAN	TCP	*	*	WAN address	25 (SMTP)	[redacted]	25 (SMTP)	SMTP
☐	WAN	TCP	*	*	WAN address	993 (IMAP/S)	[redacted]	993 (IMAP/S)	IMAP /S
☐	WAN	TCP	*	*	WAN address	587 (SUBMISSION)	[redacted]	587 (SUBMISSION)	SMTP /S

CONCLUSION

Nous avons désormais un serveur mail fonctionnel, accessible de l'extérieur et légitime auprès des autres serveurs mails.
Pour se connecter depuis un client de messagerie il faudra saisir les informations suivantes :
Adresse mail : user_NAS@domain.tld
Login : user_NAS (sans le @domain.tld)
MDP : MDP_user_NAS
Serveur entrant : mail.domain.tld
Port : 993 (TLS)
Serveur sortant mail.domain.tld
Port : 587 (STARTTLS)

Révision #5
Créé 2 mai 2020 02:39:36 par garfieldtux
Mis à jour 2 mai 2020 02:59:11 par garfieldtux