

# 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.

The screenshot shows the Synology Package Center interface. On the left, there is a navigation menu with options like 'Recherche', 'Installé', 'Mettre à jour', 'Explorer', 'Recommandé', 'Tous', 'Sauvegarder', 'Multimédia', 'Entreprise', 'Sécurité', 'Utilitaires', and 'Communauté'. The main area displays the 'Centre de paquets' for 'Mail Server'. It includes buttons for 'Installation manuelle', 'Actualiser', and 'Paramètres'. Below these, there is a 'Retour' button and an 'Action' dropdown. The status section shows: 'Statut: En cours d'exécution', 'Développeur: Synology Inc.', 'Version: 1.5-0329', 'Volume installé: volume1', and 'Nombre de téléchargement: 1,967,000+'. A 'Journal' link is also present. On the right, the 'Mail Server' configuration window is open, showing the 'SMTP' tab. It has options to 'Enable SMTP', 'Account type' (Local users), and checkboxes for 'Authorization required for mail clients except Mail Station', 'Ignore authorization for LAN connections', and 'Sender name and login name must be identical'. Fields for 'Domain name' (synology.com), 'Port' (25), and 'Maximum size per email' (10) are visible. There are also fields for 'SMTP-SSL' (Port: 465) and 'SMTP-TLS' (Port: 587). A 'Description' section at the bottom explains that the Mail Server provides a solution for sending and receiving emails on a Synology DiskStation.

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.

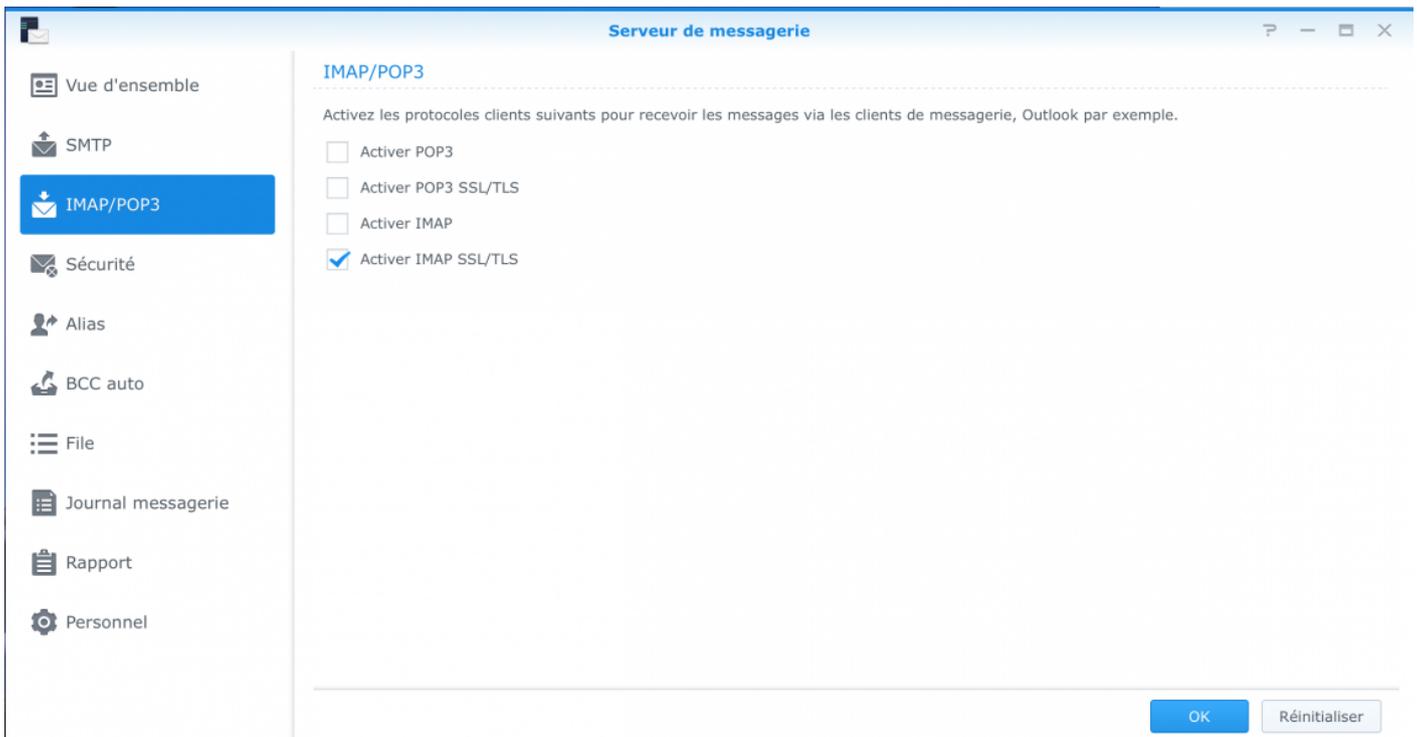
Dans le champ nom d'hôte, nous allons entrer le nom de domaine qui correspondra aux adresses mail. Ex : *domain.tld* enverra des mails en *someone@domain.tld*

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.

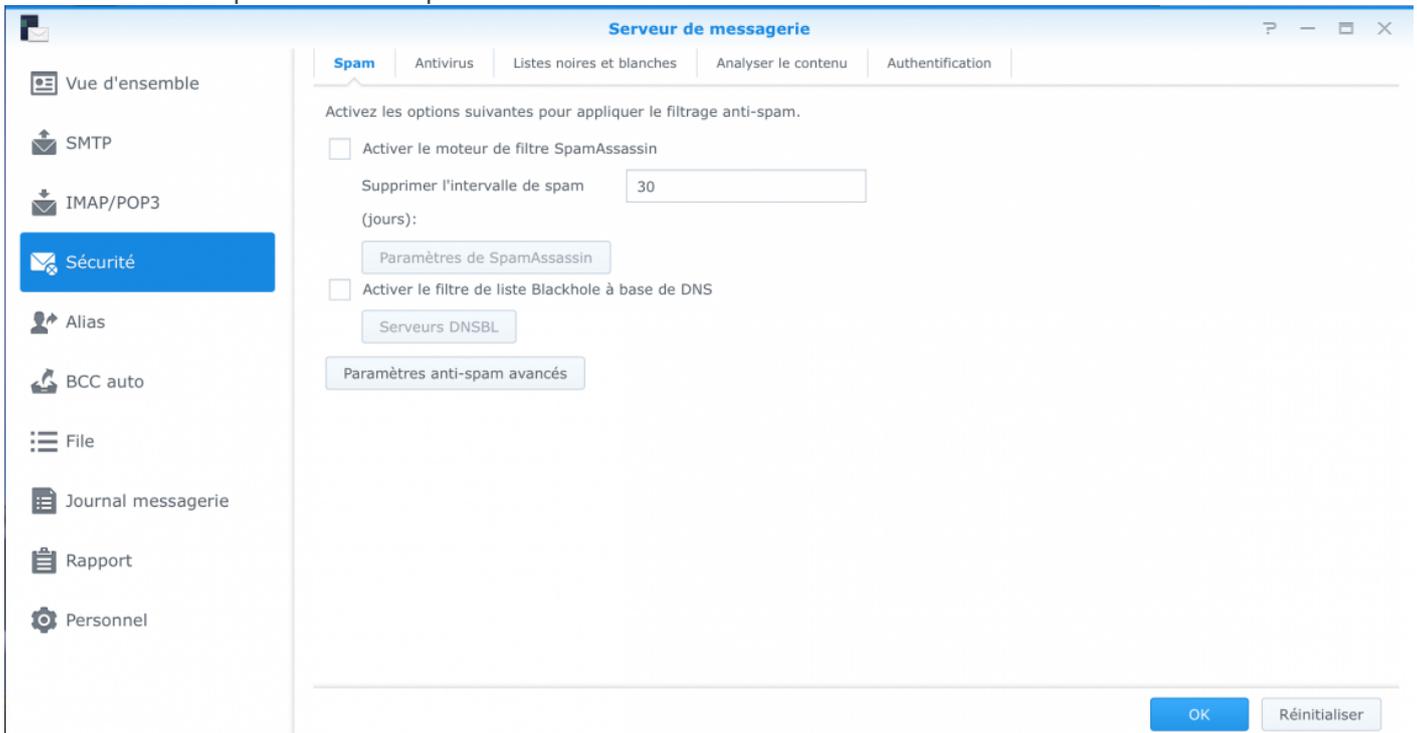
The screenshot shows the 'Serveur de messagerie' configuration window. The left sidebar has 'Vue d'ensemble', 'SMTP', 'IMAP/POP3', 'Sécurité', 'Alias', 'BCC auto', 'File', 'Journal messagerie', 'Rapport', and 'Personnel'. The 'SMTP' tab is selected. It contains the following settings: 'Activer le SMTP pour envoyer et recevoir du courrier.' with a checked 'Activer SMTP' checkbox; 'Type de compte:' set to 'Utilisateurs locaux'; 'Activer l'authentification SMTP' checked, with 'Ignorer l'autorisation pour les connexions du réseau local' and 'Le nom de l'expéditeur et le nom de connexion doivent être identiques' unchecked; 'Nom d'hôte (FQDN):' set to 'domain.tld' with an 'Additional Domain' button; 'Port:' set to '25'; 'Taille maximale par message (Mo):' set to '50'; 'Activer SMTP-SSL' unchecked, with 'Port:' set to '465'; 'Activer SMTP-TLS' checked, with 'Port:' set to '587'; and a 'Relais SMTP' button at the bottom.

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 boîtes pour une seule et même personne.

Il est également possible de renvoyer un alias sur une boîte aux lettres 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.

**Serveur de messagerie**

Créer Modifier Supprimer Outils

Recherche

Alias	Membre
abuse	
contact	
root	

1 3 élément(s)

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.

**Serveur de messagerie**

Effacer Exporter

Recherche

Message ID	Date	Heure	Expéditeur	Destinataire	Taille de ...	Statut
201603161341...	2016-03-16	14:41:16			2.8KB	Reçu
	2016-03-16	12:49:59			0.3KB	Envoyé
	2016-03-16	06:00:04			2.4KB	Envoyé
201603152231...	2016-03-15	23:34:28			0.3KB	Envoyé
201603152226...	2016-03-15	23:28:56			0.3KB	Reçu
201603152224...	2016-03-15	23:27:17			0.4KB	Reçu
67277be173ac...	2016-03-15	22:47:11			0.9KB	Envoyé
7f5da3773512c...	2016-03-15	22:27:51			12.2KB	Envoyé
a2352b9cfc5c8...	2016-03-15	22:17:54			11.8KB	Envoyé
07025f3f2aea5...	2016-03-15	20:12:50			12.3KB	Envoyé
f6d91875a12ac...	2016-03-15	20:07:51			11.9KB	Envoyé
87488544565f...	2016-03-15	20:02:50			11.9KB	Envoyé
9171290bfaf1c...	2016-03-15	19:02:50			10.9KB	Envoyé
2197df8cab5b0...	2016-03-15	18:57:52			11.0KB	Envoyé
a67d311ff66db...	2016-03-15	18:57:51			12.3KB	Envoyé
5c5add5b1beb...	2016-03-15	18:27:49			11.7KB	Envoyé
1bebd2e213f79...	2016-03-15	18:22:49			12.0KB	Envoyé

1 2 3 358 élément(s)

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

Serveur de messagerie

**Rapport**

Activer le rapport quotidien

Envoyer à : 06 : 00

Envoi à: [Champ masqué]

Fournisseur de service: Serveur SMTP personnalisé

Serveur SMTP: [Champ masqué]

Port SMTP: [Champ masqué]

Authentification requise

Compte: [Champ masqué]

Mot de passe: [Champ masqué]

Une connexion sécurisée (SSL/TLS) est nécessaire

Nom de l'émetteur: Report MailStation

Adresse email de [Champ masqué]

l'émetteur: [Champ masqué]

**Paramètres de vérification**

Vérifiez les paramètres de votre Mail Server et analysez les faiblesses potentielles.

Vérifier

OK Réinitialiser

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

Serveur de messagerie

**Personnel**

Activez les options suivantes pour appliquer les fonctions Transfert auto et Réponse auto.

Activer le Transfert auto

Transférer les messages [Champ vide]

vers:

Garder une copie des messages dans la boîte de réception

Activer la Réponse auto

Plage horaire: De [Champ vide] À [Champ vide]

Objet: This is an autoreply...[Re: \$SUBJECT]

Message: Dear \$FROM,  
Please note that I am away. Your message regarding \$SUBJECT will be read when I return. Thank you.

Paramètres avancés

OK Réinitialiser

# 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.



## Ajouter une entrée à la zone DNS

✕

Étape 2 sur 3

Sous-domaine

TTL

Cible \*   
La cible doit être une IPv4 valide.

Le champ A actuellement généré est le suivant :

```
mail IN A 11.22.33.44
```

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



## Modifier une entrée de la zone DNS



Sous-domaine

TTL

Par défaut

Priorité \*

10



Cible \*

mail.



Le champ MX actuellement généré est le suivant :

```
IN MX 10 mail.domain.tld.
```

Attention : L'édition manuelle des champs MX peut entraîner la perte d'emails !

Annuler

Suivant

# 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 enregistrements 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**.

**Serveur de messagerie**

Spam   Antivirus   Listes noires et blanches   Analyser le contenu   **Authentification**

**SPF**

SPF est un système de validation des courriers électroniques conçus pour vérifier l'identité de l'expéditeur et éviter les courriels en détectant les adresses expéditeurs forgées.

Activer la vérification SPF

Rejeter les pannes souples SPF

**DKIM**

DKIM permet aux destinataires d'utiliser une clé publique afin de valider la signature de l'expéditeur pour réduire le nombre de courriers potentiellement malveillants ou de pourriels.

Activer DKIM

Préfixe du sélecteur:

DKIM:

Clé publique:

**DMARC**

DMARC Permet aux destinataires de valider le domaine de messagerie réclamé par expéditeur.

Activer 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.



## Modifier une entrée de la zone DNS



Sous-domaine

TTL

Personnalisé

600



s.

Valeur \*

"v=spf1 a mx ip4: [redacted] ~all"

Le champ TXT actuellement généré est le suivant :

```
600 IN TXT "v=spf1 a mx ip4: [redacted] ~all"
```

Annuler

Suivant

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\_publicue*

En remplaçant bien sur *cle\_publicue* par la clé générée par Mail Server.



## Modifier une entrée de la zone DNS



Sous-domaine

TTL

Valeur \*

Le champ TXT actuellement généré est le suivant :

```
mailkey._domainkey IN TXT "t=s; p=
```

```
"
```

Annuler

Suivant

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



## Modifier une entrée de la zone DNS



Sous-domaine

`_dmarc`

TTL

Par défaut

Valeur \*

`"v=DMARC1; p=none"`

Le champ TXT actuellement généré est le suivant :

```
_dmarc IN TXT "v=DMARC1; p=none"
```

Annuler

Suivant

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.

<input type="checkbox"/>		WAN	TCP	*	*	WAN address	25 (SMTP)		25 (SMTP)	SMTP	
<input type="checkbox"/>		WAN	TCP	*	*	WAN address	993 (IMAP/S)		993 (IMAP/S)	IMAP /S	
<input type="checkbox"/>		WAN	TCP	*	*	WAN address	587 (SUBMISSION)		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