

LIVRE BLANC

COMMENT INTERNALISER
VOTRE ROUTAGE EMAIL ?



DeliverNow



TABLE DES MATIÈRES

Introduction	3
1 Pourquoi vouloir changer votre architecture délivrabilité ?	3
1.1. Réputation d'expéditeur	3
1.2. Gestion des incidents de délivrabilité	3
1.3. Manque de réactivité de la part de votre prestataire	4
1.4. Renforcement de la sécurité de votre infrastructure	4
1.5. Contraintes liées à l'internalisation	5
2 Les différentes étapes	5
2.1. Choisir la bonne solution.....	5
2.1.a. Une solution opensource ou propriétaire ?	5
2.1.b. Quels sont les critères qui devraient influencer votre choix ?	5
2.1.c. Le choix de DeliverNow : PowerMTA	6
2.2. Répertorier les différents flux email.....	7
2.3. Configurer l'infrastructure	7
2.3.a. Analyse	7
2.3.b. Installation des différentes briques.....	7
2.3.c. Configuration de la délivrabilité.....	8
2.3.d. Formation des équipes	8
2.3.e. Test unitaire.....	8
2.3.f. Mise en production et chauffage des adresses IP	8
3 Monitoring de la réputation et de la délivrabilité	9
3.1. Quelles sont les différentes données permettant le monitoring de la réputation ? ..	9
3.2. Comment bâtir le bon outil de monitoring ?	9
3.3. La Deliverability Monitoring Suite de DeliverNow	10
3.4. La mise en place du pupitre DMS	11
4 Quelles sont les différentes responsabilités dans une organisation délivrabilité ?	11
5 Comment DeliverNow peut vous aider ?	12
Nous contacter	14

Introduction

Au fil des ans, la délivrabilité est devenue un point stratégique pour toute entreprise exploitant l'email marketing. Pour diverses raisons, le sujet est devenu de plus en plus complexe : augmentation du nombre d'attaque de phishing, plus grande agressivité des filtres anti-spam, boîtes email intelligentes, internationalisation des listes d'email...

Dans ce livre blanc, nous prendrons le temps de vous expliquer pourquoi l'internalisation de la délivrabilité est une piste à envisager afin de mieux maîtriser ces défis. Nous vous guiderons aussi dans les grandes étapes qui vous permettront de mener à bien un projet d'internalisation, que ce soit dans la mise en place technique ou dans les évolutions à mener au sein de votre organisation.

1 Pourquoi vouloir changer votre architecture délivrabilité ?

L'INTERNALISATION DE LA DÉLIVRABILITÉ N'EST PAS UNE RECETTE MAGIQUE QUI VOUS ÉVITERA TOUS LES PROBLÈMES. MAIS SI LA DÉLIVRABILITÉ EST STRATÉGIQUE POUR VOTRE ACTIVITÉ, VOUS AVEZ TOUT INTÉRÊT À IMPLIQUER VOS ÉQUIPES INTERNES DANS SA MAÎTRISE.

1.1. Réputation d'expéditeur

Internaliser la délivrabilité, cela veut dire ne pas dépendre de la réputation globale d'un routeur ou même de la réputation des autres clients de ce routeur. En utilisant votre propre infrastructure, votre propre range d'adresses IP, votre propre nom de domaine... vous êtes certain que votre réputation d'expéditeur dépend à 100% de vos pratiques.

D'autre part, en cas de problème, l'analyse de votre réputation n'est pas perturbée par des éléments extérieurs, non maîtrisés.

1.2. Gestion des incidents de délivrabilité

Lorsque vous utilisez un routeur tiers et qu'un incident de délivrabilité survient, la méthode d'escalade classique commence quasi systématiquement par un système de support client par ticket. Malheureusement, il est rare que la personne avec qui vous êtes en contact ait toutes les informations et les connaissances suffisantes afin de vous aider à résoudre votre problème. Dans la plupart des cas, il faudra qu'un second niveau de support intervienne avec des temps de réponses largement insuffisants face à l'importance stratégique des questions de délivrabilité pour votre entreprise.

Les avantages de l'internalisation sont ici flagrants :

- Vous avez l'ensemble des **logs à portée de main**, vous permettant d'analyser chaque étape du dialogue SMTP (HELO, MAIL FROM, RCPT TO, DATA, ...) ;
- Vous maîtrisez **vos infrastructure et son monitoring technique**. Vous êtes donc capable d'identifier les incidents internes qui pourraient survenir (perte de connectivité, problème de réactivité d'un serveur, ...) ;
- L'ensemble des connaissances et des données sont à portée de main. Cela vous permet de réduire drastiquement les délais de résolution des incidents **en mobilisant vos équipes internes**.

1.3. Manque de réactivité de la part de votre prestataire

Comme on l'a déjà vu au point précédent, le routage via un tiers comporte un inconvénient majeur qui est le manque de réactivité potentiel des équipes de support et des équipes délivrabilité. Les spécialistes délivrabilité sont extrêmement rares sur le marché de l'emploi. Chez chaque routeur on peut compter entre un et trois (rarement plus) « deliverability managers », c'est à dire des personnes dédiées à la mise en place, à la gestion, et à la surveillance de la délivrabilité. En faisant un calcul simple, suivant le nombre de clients de votre routeur, essayez de deviner combien de temps un deliverability manager aura l'occasion d'accorder à chaque client ? En général, ce sera beaucoup moins d'une heure par mois autant dire pas grand-chose, surtout en cas d'incident majeur.

En cas d'internalisation, vous pouvez réinvestir les économies réalisées sur les licences, les coûts à l'envoi et les coûts d'intégration dans la formation de vos équipes internes à ces questions ou dans un service de monitoring spécialisé tel que proposé par DeliverNow.

1.4. Renforcement de la sécurité de votre infrastructure

Quand vous exploitez une base de données à des fins marketing, celle-ci constitue une richesse importante pour votre entreprise. Le temps passé et les moyens investis afin d'établir une relation de confiance avec vos clients sont inestimables. Pour cette raison, vous devriez toujours être méfiant quand il s'agit de confier votre base de données à un tiers, même si c'est bien souvent pour une très bonne raison. Avec l'externalisation de votre délivrabilité, c'est non seulement votre liste d'email que vous confiez à un tiers, mais c'est aussi l'ensemble de vos messages et des données comportementales générées par ceux-ci.

En internalisant, vous serez aussi obligé d'internaliser toutes les questions de sécurité des données et de gestion des adresses email. Si cela peut sembler un chantier considérable, c'est aussi un avantage important parce que vous avez l'occasion de réduire le nombre d'intervenants et donc la fiabilité de vos protocoles de sécurité.

1.5. Contraintes liées à l'internalisation

Pour autant, si l'internalisation a de nombreux avantages, elle comporte aussi son lot de contraintes. Vous devrez mobiliser des ressources plus importantes, tant au niveau technique que des ressources humaines. L'internalisation a donc un coût, qu'il faudra évaluer face à l'option de l'externalisation.

D'autre part, en internalisant votre délivrabilité, vous aurez aussi une responsabilité vis-à-vis de l'écosystème. Cette responsabilité n'est pas à négliger, vous deviendrez le seul responsable face à de possibles dérives liées à une mauvaise exploitation du canal email et aurez l'obligation de les détecter, et le cas échéant de les juguler.

2 Les différentes étapes

2.1. Choisir la bonne solution

2.1.a. Une solution opensource ou propriétaire ?

Il existe sur le marché de très nombreux MTA (Mail Transfer Agent), vous devriez donc forcément y trouver votre compte. On peut séparer ce marché en deux grandes catégories, d'une part les MTA Opensource (certains disposant aussi d'une version commerciale, comme Sendmail) et d'autre part, les MTA propriétaires. Le premier critère de différenciation entre ces deux catégories est bien entendu le prix, mais il ne faut pas oublier d'évaluer aussi l'importance du support et de la rapidité avec laquelle les mises à jour sont distribuées.

Opensource

- Postfix : www.postfix.org
- Exim : www.exim.org
- Sendmail : www.sendmail.com/sm/open_source/
- MantaMTA : <http://manta.io/>

Propriétaire

- MessageSystems : www.messagesystems.com
- MailerQ : www.mailerq.com/
- PowerMTA : www.port25.com

2.1.b. Quels sont les critères qui devraient influencer votre choix ?

Voici une série de critères sur lesquels vous devriez vous baser afin de faire un choix éclairé concernant le MTA qui convient le mieux à vos besoins :

- Est-ce que l'argument du prix est vraiment déterminant au regard du chiffre d'affaire généré par l'email dans mon entreprise ? Quel est le ROI de la mise en place d'un MTA performant ?

- Est-ce que les technologies (et dépendances) requises par ce MTA sont maîtrisées par mes équipes ?
- Quel est le niveau de support dont j'aurai besoin en cas d'incident technique majeur ? Est-ce qu'il est possible d'obtenir un SLA de la part de ce vendeur ? Si ce n'est pas le cas, est-ce que mes équipes internes sont capables de gérer ces questions ?
- Quel est le niveau de monitoring pris en charge directement par le MTA ? Comment sont gérées les alertes en cas d'incident technique ou de délivrabilité ?

2.1.c. Le choix de DeliverNow : PowerMTA

Chez DeliverNow, nous avons fait le choix de privilégier PowerMTA (et de devenir revendeur et intégrateur agréé), une solution éditée depuis 1999 par Port25.



PowerMTA équipe aujourd'hui la majeure partie des grands routeurs internationaux c'est une solution qui a fait ses preuves et dont la robustesse n'est plus à prouver :

- Authentification et gestion des flux. PowerMTA propose un mode « Guaranteed Authentic » qui certifie la qualité des signatures de vos emails et déclenche des alertes en cas d'échec. Via des MTA virtuels, PowerMTA permet aussi de gérer un nombre illimité d'adresses email et de séparer les différents flux d'emails en fonction de l'importance accordée à chaque type de message.
- Gestion de la connectivité. L'outil permet aussi une gestion fine des paramètres de connexion aux différentes destinations/noms de domaine, par exemple, nombre de connexions simultanées, nombre de messages par connexion, nombre de tentatives par heure, durée maximale des « retry », différenciation des méthodes d'authentification à utiliser, ...
- Suivi de la délivrabilité. PowerMTA vous permet de suivre l'évolution de votre délivrabilité, par destination, par campagne, ou par MTA virtuel :
 - Catégorisation en temps réel des bounces ;
 - Outils d'analyse des statistiques en ligne de commande ;
 - Accès aux statistiques via une interface web ;
 - Gestion des exports des logs dans différents formats (XML, CSV, HTML, ...) ;
 - Une API permettant de brancher vos logs sur votre propre système d'analyse.

Note : Le choix de PowerMTA comme outil de prédilection ne nous empêche absolument pas de travailler avec les autres solutions du marché si elles s'avèrent plus intéressantes pour votre cas particulier.

2.2. Répertoire des différents flux email

C'est une étape qui est trop souvent négligée, mais il est indispensable de passer par une phase de recherche de tous les flux emails sortant de l'entreprise. Trop souvent, surtout si votre activité a un long historique, vous vous rendez compte que vos flux emails sont routés par différentes plateformes qui sont venues s'ajouter au fil du temps et des changements de responsables.

Cette situation peut être préjudiciable quand ces différents environnements de routage sont en conflit, ne respectent pas les règles élémentaires d'authentification ou, pire encore, ont été oubliés.

Le changement de plateforme, ici pour une internalisation, est l'occasion de référencer précisément ces différents flux afin de n'en oublier aucun lors de votre migration.

2.3. Configurer l'infrastructure

2.3.a. Analyse

La configuration de votre infrastructure devra toujours commencer par une analyse permettant de correctement dimensionner celle-ci. Dans cette analyse plusieurs paramètres entrent en compte :

- Volume quotidien « moyen » d'emails à envoyer
- Anticipation de pics pouvant provenir dans votre trafic afin que l'infrastructure tienne la charge dans ces conditions
- Analyse des performances attendues
- Analyse des contraintes spécifiques liées à votre business
- Analyse de l'architecture technique existant et des technologies utilisées
- Moyens humains et connaissances en présence

2.3.b. Installation des différentes briques

La première étape est évidemment la préparation de l'architecture serveur. Vient ensuite l'installation des différentes couches de l'infrastructure :

- CMS – outil de gestion de campagne
- MTA – Mail Transfert Agent
- Les outils de surveillance de la délivrabilité

Ces différentes couches doivent ensuite être configurées et interconnectées afin de pouvoir interagir entre elles.

2.3.c. Configuration de la délivrabilité

On peut distinguer plusieurs éléments différents dans la configuration de la délivrabilité.

La première étape consiste à configurer les adresses IP et les noms de domaine au niveau du MTA et des enregistrements DNS.

La seconde étape vise à configurer les différentes technologies d'authentification qui sont un élément primordial de la délivrabilité :

- SPF : Sender Policy Framework
- DKIM : DomainKey Identified Mail
- DMARC : Domain-based Message Authentication, Reporting & Conformance

La configuration de ces trois technologies se fait principalement via des enregistrement DNS, mais aussi via de la configuration du MTA, et pour DMARC, la configuration d'outils de monitoring des feedbacks.

Enfin, il faudra configurer les sources externes de gestion de la réputation et les interconnecter avec les outils de monitoring. On peut citer :

- Les boucles de rétroaction (Hotmail, AOL, Yahoo !, SignalSpam, ...)
- Le monitoring des blacklists
- La configuration des différents centres de monitoring gérés par les FAI (SNDS pour Outlook.com, Mail.ru, ...)

Si cela vous concerne, le whitelisting de vos IPs pourra aussi être un élément à mettre en place à cette étape du processus d'internalisation.

2.3.d. Formation des équipes

C'est une étape essentielle à ne surtout pas négliger dans la mise en place de votre infrastructure. Cela vous garantira une maîtrise des différents outils par vos équipes et de pouvoir réagir plus efficacement en cas d'incident.

2.3.e. Test unitaire

C'est un passage obligé dans le déploiement des différentes briques de la solution. Il est important pour les tests de s'entourer de spécialistes qui vous fourniront une méthodologie de test éprouvée.

2.3.f. Mise en production et chauffage des adresses IP

Si les adresses IP que vous avez configurées n'ont jamais été utilisées pour envoyer du trafic email, on considère que celles-ci ont une réputation neutre vis-à-vis des FAI. Les spammeurs

changeant régulièrement d'adresses IP afin d'échapper au filtrage, les FAI font très attention aux adresses IP neutres et il convient donc de démarrer les envois en douceur. C'est que l'on appelle le Warmup, ou encore le Rampup.

Afin que vos adresses IP puissent se bâtir une réputation positive, il est important de faire très attention à cette phase de Warmup. Votre programme email devra faire ses preuves, c'est-à-dire prouver que vos destinataires réagissent positivement à vos communications.

3 Monitoring de la réputation et de la délivrabilité

3.1. Quelles sont les différentes données permettant le monitoring de la réputation ?

Ce n'est un secret pour personne, envoyer des emails génère de très nombreuses données. Ce volume est d'ailleurs en train de gonfler en même temps que l'évolution de la sophistication des stratégies email marketing. En plus des données issues du tracking des clics et des ouvertures, on peut par exemple évoquer les données générées par la géolocalisation, l'analyse comportementale, ... Mais le plus grand générateur de données en email marketing reste le protocole SMTP lui-même. Chaque connexion SMTP étant constituée d'un dialogue entre deux serveurs SMTP distants, les étapes de ce dialogue génèrent une quantité de « traces » impressionnante.

Pour correctement analyser et suivre l'évolution de la délivrabilité, l'utilisation des données internes (issues du tracking et de SMTP) n'est pas suffisante. Il faut savoir exploiter et réintégrer les données issues de systèmes externes, par exemple :

- Le traitement et l'analyse des données issues des boucles de rétroaction (le nombre de plaintes par adresse IP) ;
- Les données issues du monitoring des listes noires ;
- Les informations concernant le nombre de spamtraps touchés ;
- Les données proposées par les « fournisseurs » de réputation comme Senderscore de Return-Path ou Senderbase de Cisco ;

3.2. Comment bâtir le bon outil de monitoring ?

Les données provenant des différentes sources de réputation étant totalement hétérogènes, la seule solution efficace consiste à construire un système de monitoring via l'analyse des logs des différentes couches logicielles présentes dans l'infrastructure délivrabilité. Fichiers de logs qui seront croisés avec les sources de réputation externes à disposition.

Sur cette base, il sera nécessaire de créer des alertes afin de pouvoir réagir le plus rapidement possible en cas d'incident.

Malheureusement, la conception d'un dashboard de monitoring est un travail ardu qui nécessite beaucoup de temps et d'expertise. Afin de répondre à ce besoin, DeliverNow a construit une solution « prête à déployer ».

3.3. La Deliverability Monitoring Suite de DeliverNow

DeliverNow a décidé de s'appuyer sur les services de Splunk en devenant revendeur agréé. Splunk est un moteur de collecte, d'indexation et d'exploitation des données générées par les différents composants d'une infrastructure informatique. L'outil permet de déployer des solutions de monitoring permettant de détecter et de diagnostiquer tout incident pouvant survenir dans l'exploitation d'une infrastructure informatique.



Sur base de Splunk, DeliverNow a développé une solution clé en main (lié à l'utilisation de PowerMTA de Port25 ou à d'autres MTA) vous permettant d'avoir une maîtrise complète de votre délivrabilité. Grâce à la Big Data, nous sommes capables de monitorer l'ensemble des paramètres constituant votre délivrabilité et de détecter dans un temps record tout incident ou toute fluctuation majeure de votre réputation d'expéditeur.

L'ensemble du dispositif DMS est le résultat de plus de trois ans de R&D et permet :

- Le monitoring de la délivrabilité sur des indicateurs accessibles par votre équipe
- La détection de problèmes de délivrabilité en temps réel
- La génération d'alertes délivrabilité suivant une trentaine de règles paramétrables
- Le suivi des incidents délivrabilité (système de tickets), regroupés dans quatre grandes catégories
- Le reporting des indicateurs de performance délivrabilité dans dix tableaux de bord synthétiques

La prestation de DeliverNow comprend la mise en place des outils, le paramétrage des tableaux de bord en fonction des spécificités des campagnes emailing que vous menez. En fonction de vos besoins, est ensuite mise en place :

- Une réunion mensuelle avec vos équipes pour vous guider dans les actions prioritaires à mener pour améliorer votre délivrabilité
- Un suivi mensuel de votre responsable délivrabilité pour l'aider à prendre en main les différents outils et monter en compétences.

3.4. La mise en place du pupitre DMS

Voici ci-dessous les différentes étapes du déploiement de DMS afin de surveiller au mieux votre infrastructure délivrabilité :

- **Installation du framework Splunk** sur vos serveurs
- **Installation de l'application DMS** par l'équipe de DeliverNow
- Configuration des sources de **données SMTP venant de votre MTA**
- Configuration des sources de **données de tracking** provenant de votre outil de gestion de campagne
- Configuration des sources de **données « seeding »** de DeliverNow : système permettant de mesurer le taux de placement de vos emails en boîte principale.
- Configuration des **sources de données externes** : réputation SNDS, blacklists, feedback loops...
- **Mise en place des alertes** et formation de vos équipes

4 Quelles sont les différentes responsabilités dans une organisation délivrabilité ?

À la frontière de la technique et du marketing, la délivrabilité se trouve sans cesse confrontée à un dilemme quant aux responsabilités des uns et des autres. Nous n'allons pas ici tenter de définir finement qui est responsable de quoi, mais plutôt dégager quatre grands domaines de responsabilité.

Ces grands domaines de responsabilité doivent ensuite se trouver un responsable qui pourra avoir différents visages en fonction de votre organisation.

- **Configuration et monitoring technique** : C'est la plus évidente des 4 grandes responsabilités en matière de délivrabilité. Il s'agit ici de configurer, faire évoluer et surveiller l'infrastructure technique vous permettant de délivrer vos emails.
- **Monitoring de la réputation** : Surveiller la réputation de vos adresses IP et de vos noms de domaine n'est pas réellement une compétence technique ou business. Pour autant, c'est un point crucial de votre organisation. Chaque signal, alerte, doit être pris en considération et interprété correctement.
- **Relation FAI** : En cas d'incident, lorsque cela se justifie, il faut savoir prendre contact avec les FAI et les webmails pour résoudre certains blocages. Ici, le plus important est d'avoir une parfaite compréhension des règles (parfois tacites) qui régissent le monde de la délivrabilité et du filtrage du spam. Il est important aussi de connaître les grands acteurs, leurs organisations et les différents canaux afin de communiquer le plus efficacement avec ceux-ci.
- **Responsabilité Marketing/Business** : La plupart des incidents de délivrabilité sont provoqués par des décisions business. Que ce soit par des méthodes de collecte d'adresses non maîtrisées ou par une gestion des données (bounce, désinscription, plaintes, segmentation, ...) imparfaites.

5 Comment DeliverNow peut vous aider ?

Afin de répondre aux différents besoins en matière d'internalisation de la délivrabilité, DeliverNow a créé une solution totalement intégrée répondant à l'ensemble de vos besoins.

Cette solution, c'est iES! (In-House Emailing Suite) :



- Un **campaign management system** professionnel vous permettant de remplir tous les besoins de vos équipes marketing. Cela va de la gestion de liste, à la gestion de templates email en passant par la segmentation et la création de landing pages et d'enquêtes (voir schéma p. 13 pour retrouver l'ensemble des fonctionnalités).
- Spécialisé depuis plusieurs années dans le déploiement des **solutions de routage basées sur PowerMTA**, DeliverNow vous propose de mettre en place cette solution leader du marché de la délivrabilité et utilisée par les plus grands routeurs d'emails dans le monde.
- **Le monitoring de la délivrabilité** et de la réputation d'expéditeur est une affaire de spécialistes. Avec iES, vous suivez en temps réel le placement en inbox de vos emails, la disponibilité de vos ressources délivrabilité, la réputation de vos domaines et de vos adresses IP, ...
- Avec iES, vous avez aussi accès en permanence aux conseils de votre **Deliverability Manager**. Celui-ci sera capable d'intervenir en cas de questions et d'optimiser votre infrastructure lorsque vous ferez face à de nouveaux défis ou que vos besoins évolueront.



iES! in-House Emailing Suite

Campaign Manager



CMS

Campaign Management System

- ✓ List management
- ✓ Segment management
- ✓ Email Management
- ✓ WYSIWYG Editor
- ✓ Email templates management
- ✓ Email Marketing Reports
- ✓ Autoresponders and Triggers
- ✓ Survey and feedback forms
- ✓ Personalization
- ✓ Open and link tracking
- ✓ Google Analytics Integration

MTA

Mail Transfert Agent

- ✓ Connectivity management
- ✓ Virtual MTA management
- ✓ Queue prioritization
- ✓ Bounce management
- ✓ Feedback loop management
- ✓ Authentification management
- ✓ API connectivity
- ✓ IPv6 support
- ✓ SNMP support

ISPs
and
Webmails

Deliverability Manager




DMS

Deliverability Monitoring Suite

- ✓ Deliverability monitoring dashboards
- ✓ Deliverability alerts and tickets
- ✓ Mailbox monitoring
- ✓ Reputation monitoring
- ✓ IPs et domains monitoring
- ✓ Deliverability management workflow
- ✓ Deliverability ressources
- ✓ Management reports



Nous contacter



DeliverNow



48 rue sarrette
75685 Paris Cedex 14
Tel. : 01 75 43 46 78
contact@delivernow.eu



https://twitter.com/delivernow_



<https://www.facebook.com/pages/DeliverNow/434748366608178>



<https://www.linkedin.com/company/delivernow>



<http://fr.viadeo.com/fr/company/delivernow>