Traduction de la documentation en ligne de `Postfix`

Olivier « Oluve » Le Monnier
Administrateur Système et Réseau
CRDP de Basse-Normandie
Ingénierie Éducative

`Postfix` est le système de courrier de *Wietse Venema*, également auteur des *wrapper tcp*, reconnus pour leur intérêt dans le domaine de la sécurité, et pour la qualité du code par toute la communauté des logiciels libres.

Les 100 millions d'utilisateurs utilisant l'Internet envoient environ 1000 milliards de méls par jour. L'objectif à la conception de `Postfix` était de réaliser un système de courrier alternatif à `Sendmail`, qui soit rapide, facile à administrer et sécurisé tout en étant autant que possible compatible avec *Sendmail*.

Présentation générale

Objectifs et fonctionnalités

Objectifs principaux

Large diffusion

pour que l'impact sur les performances de l'Internet soit sensible il faut que `Postfix` soit largement diffusé. C'est pourquoi c'est un logiciel libre ;

Performance

`Postfix` est trois fois plus rapide que son plus proche « rival » (`Qmail`). Des « trucs » utilisés pour les serveurs *Web* sont exploités pour réduire la création de processus, et d'autres types de « trucs » permettent de réduire l'utilisation du système de fichiers, tout ça sans diminution des performances ;

Compatibilité

la migration de `Sendmail` devant être facile, les fichiers `/var/spool/mail`, `/etc/aliases`, et `~/.forward` sont utilisés. Toutefois, l'administration devant être simple, il n'existe pas de fichier [2]`sendmail.cf` ;

Sûreté et robustessse

si le système n'a plus de mémoire ou d'espace disque, `Postfix` n'endommagera pas les choses d'avantage, il a été conçu pour rester sous contrôle ;

Flexibilité

`Postfix` est conçu de façon modulaire. Une douzaine de petits programmes assurent chacun une tâche spécifique. Il est possible de remplacer les programmes par défaut par des produits maison, voire de supprimer certains programmes inutiles dans certains cas ;

Sécurité

chaque programme est enfermé (*chrooté*), il n'y a aucun lien direct entre le réseau et les programmes sensibles comme la livraison du courrier local. `Postfix` ne fait même pas confiance à ses propres files de courier. De plus, aucun des programmes n'a besoin des droits *root* (*setuid*).

Autres fonctionnalités intéressantes

Différentes solutions de transport

outre smtp, il est possible d'implémenter d'autres solutions de transport des messages comme uucp, [2]*DECnet* ou *X400* ;

Domaines virtuels

le changement d'une seule tables suffit à ajouter un domaine virtuel au système de courrier, là où plusieurs niveaux d'alias et de redirections sont nécessaires avec d'autres systèmes ;

Contrôle uce

les suspects usuels sont reconnus, rbl, requêtes dns sur les adresses expéditeurs. Le contrôle du contenu n'est pas encore implémenté ;

Tables

`Postfix` ne comprend pas encore de langage de réécriture des adresses mél, a la place un usage extensif de requêtes sur des tables db, dbm et nis est réalisé.

Architecture globale

Introduction

Certains systèmes de courrier comme `Sendmail` sont implémentés sous la forme d'un seul programme monolithique qui se charge de tout. Il est facile dans cette configuration de partager les données entre différentes parties du programme, mais il est aussi facile de faire des erreurs fatales.

D’autres systèmes utilisent une hiérarchie rigide de programmes qui permet l’utilisation des programes dans un ordre clairement défini. Cette approche permet une meilleure isolation des éventuels problèmes au prix d’un plus grand nombre de processus et d’une communication inter-processus plus importante.

Ce prix peut être maintenu dans une marge acceptable en tronçonnant la fonction globale assez finement.

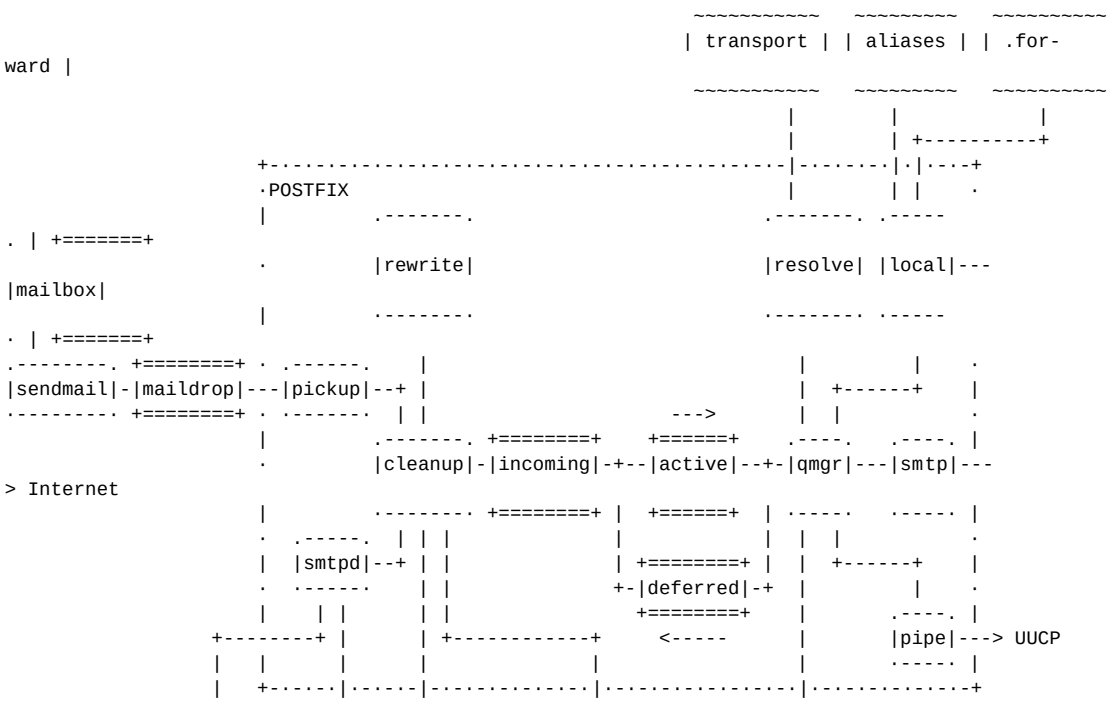
Architecture

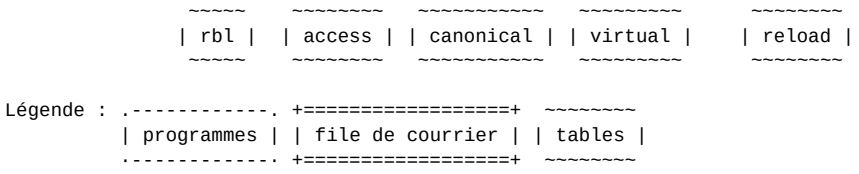
`Postfix` est basé sur des programmes semi-residents, coopérant, assurant chacun une tâche précise, sans relation de parent-enfant entre eux. L’un des avantages est de rendre chaque service, comme la réécriture des adresses par exemple, disponible à tous les proccessus sans augmenter le nombre de processus.

Un démon-maître résident se charge de lancer les différents programmes en fonction des besoins. Ces processus peuvent être dupliqués un nombre configurable de fois, sont réutilisables un nombre configurable de fois et s’arrêteront au bout d’un temps configurable également. Cette méthode réduit de manière drastique la création de processus, tout en fournissant une bonne isolation entre les programmes.

L’intérêt est de pouvoir facilement réduire l’architecture au strict minimum.

Schéma structurel





Les éléments suivants ne sont pas représentés :

Les utilitaires en ligne de commande ;
Le démon-maître résident ;
Les requêtes dns effectuées par les client et serveur smtp ;
Le démon `bounce or defer et le flux de méls associés`
Les requêtes de réécriture et de résolution effectuées par le serbeur smtp et l'agent de livraison local ;
Le flux de méls délivrés localement ;
Le flux de méls envoyés au `postmaster ;`
Les signaux destinés au démons `pickup et queue manager les informant de l'arrivée de données dans les files res`

Communication inter-processus

À des fins de confidentialité, les processus communiquent via des piles fifo ou des *sockets* du type *unix-domain*, placés dans un répertoire protégé.

La quantité d'information passée entre les processus se limite bien souvent au nom d'un fichier file et à une liste de destinataires, ou à une information sur le statut du programme.

Pour éviter tout perte d'informations, `Postfix` utilise les mécanismes habituels pour s'assurer de la transmission des données, *flush*, *fsync()*, analyse des résultats d'appels système.

Gestion des files

Files de courrier

`Postfix` a quatres files de courrier : `maildrop`, `incoming`, `active` et `deferred`. Le courrier posté localement est déposé dans `maildrop`, puis envoyé dans `incoming` après nettoyage. La file `incoming` sert au courrier en cours d'arrivée ou que le gestionnaire de files (`queue manager`) n'a pas encore traité. La file `active` a une taille limitée et est ouverte par le gestionnaire de file pour la livraison. Le courrier qui ne peut pas être livré est placé dans la file `deferred` afin de ne pas entraver le reste de la livraison.

Le gestionnaire de files ne garde en mémoire que les informations concernant la fila `active`. La taille de cette file est limitée car le gestionnaire de files ne devrait jamais se trouver à cours de mémoire à cause d'un pic du trafic de courrier. Dès qu'il y a de la place dans la file `active`, le gestionnaire de files y laisse entrer un message de la file `incoming`, puis un message de la file

deferred. Cette méthode garantit le passage des nouveaux même lorsque la file deferred est particulièrement longue.

Pas de tempête de messages

Postfix essaye d'être un bon voisin. Quand il délivre un mél à un site distant, Postfix n'établiera pas plus de deux connexions pour commencer. Tant que les livraisons réussissent, le nombre de connexions augmente jusqu'à une limite configurable (ou que le réseau soit saturé) et diminue en cas de problèmes.

Gentillesse

La stratégie de livraison tient compte des domaines. Le gestionnaire de files trie les messages de la file active et envoie tous les messages par domaine de façon à maintenir les connexions smtp aussi occupée que possible.

Quand les messages arrivent plus vite qu'ils ne partent, Postfix donne la priorité aux nouveaux messages. L'idée est que les messages les plus récents doivent être délivrés avec le plus court délai, alors que les messages les plus anciens sont délivrés lorsque l'activité réduit.

Archivage exponentiel

Postfix implémente un archivage exponentiel. Quant un message n'est pas délivré à la première tentative, le gestionnaire de files marque ce message à une date future (le décalage est paramètrable). Les messages ayant cette date future sont ignorés par le gestionnaire de files.

Si la deuxième tentative échoue, une nouvelle marque est posée, le décalage correspondant au double de l'âge du message. Ainsi, le temps écoulé entre deux tentatives double à chaque échec. Cette méthode qui s'appelle l'archivage exponentiel.

Mémoire du statut des destinations

Le gestionnaire de files maintient une liste limitée, à court-terme, de destinations inaccessibles. Cette liste permet d'éviter des tentatives de livraison qui échoueraient. Cette fonctionnalité montre tout son intérêt lorsque les messages archivés pour cette destination sont nombreux.

Sécurité

Introduction

Par définition, les programmes de courrier traitent des informations provenant de sources potentiellement dangeureuses. Un système de courrier doit donc être écrit avec une grande attention quant il utilise les droits d'un utilisateur, cela même s'il n'est pas directement connecté à un réseau.

Postfix est un système complexe. La première version comprenait 30000 lignes de code, sans compter les commentaires. Avec un programme aussi complexe, la sécurité du système ne doiot pas dépendre d'un seul mécanisme. Sinon, une seule suffirait à rendre vulnérable l'ensemble du logiciel. Postfix utilise donc plusieurs couches de défense contre des erreurs logicielles ou autres.

Le moindre privilège

La plupart des démons de Postfix peuvent être lancés avec de moindres privilèges et dans un environnement fermé (*chroot*). Cela est plus particulièrement vrai pour les programmes directement exposé au réseau, comme les serveur et client smtp. Bien que l'enfermement et les privilèges les plus bas ne soient pas suffisants pour assurer une sécurité absoluement parfaite, cela y contribue fortement.

Isolation

Postfix utilise des processus différents afin d'isoler les activités de chacun. En particulier, il n'y a aucun lien entre le réseau et les programmes de livraison local particulièrement sensibles en terme de sécurité. Un intrus devra passer au travers de plusieurs programmes pour arriver à ce niveau. Certaines parties du système Postfix sont *multi-thread*ées, toutefois, aucune des parties en contact direct avec le réseau ne l'est. La séparation des processus fournit une bien meilleure isolation que le *multi-thread* utilisant un espace de nom commun.

Environnement controllé

Aucun des programmes de livraison de Postfix ne nécessite de droits utilisateur. Au lieu de cela, la majorité des programmes Postfix fonctionne sous le contrôle du démon-maître résident qui lui-même est dans un environnement controllé, sans aucune relation parent-fils avec un quelconque processus utilisateur. Cette méthodologie permet d'exclure tout exploit utilisant les fichiers ouverts, les signaux, les variables d'environnement que les systèmes Unix passent de parents éventuellement mal-intentionnés à leurs processus fils.

Droits *root*

Aucun programme postfix ne nécessite les droits de l'administrateur. L'introduction de ce concept a été la plus grosse erreur de l'histoire d'Unix. *Set-uid* pose bien plus de problèmes q'il n'en résoud. Chaque fois qu'une nouvelle fonctionnalité a été ajouté au système Unix, *set-uid* a entrainé un problème de sécurité : librairies partagées, système de fichiers /proc, support multi-langage, pour n'en mentionner que quelques-unes. De plus, *set-uid* rend impossible l'utilisation de fonctionnalités

qui ont rendus les successeurs d'Unix si attractifs, comme plan9 et les espaces de noms du système de fichiers par processus.

Par défaut, le répertoire de la file maildrop est accessible en écriture au monde entier, afin que les différents processus locaux puissent poster leurs courriers sans requérir l'assistance d'une comande *set-uid* ou du démon serveur de courrier. Ce répertoire n'est pas utilisé pour les messages venant du réseau et les fichiers de files ne peuvent pas être lus par les autres utilsateurs.

Un répertoire accessible en écriture offre des possibiltés en terme de vulnérabilité : un utilisateur local peut faire des liens durs vers les fichiers de file d'un autre utilisateur afin que cette file ne soit jamais libérée et/ou que ses messages soient livrés plusieurs fois ; un utilisateur local peut remplir le répertoire de la file maildrop de cochoneries et essayer de faire planter le système ; un utilisateur local peut aussi faire des liens durs vers les fichiers de quelqu'un d'autre pour se les faire délivrer par mél. Toutefois, les fichiers de files Postfix ont un format particulier ; la probabilité qu'un fichier non-Postfix soit reconnu comme tel est de moins d'un sur 10 puissance 12.

Si le fait que le répertoire de la file maildrop soit accessible en écriture au monde entier vous semble inacceptable, vous pouvez ne pas utiliser cette solution, révoquez les droits sur le répertoire et préférez l'activation des privilèges set-gid à un petit programme fourni pour permettre aux processus locaux d'envoyer leurs messages.

Confiance

Les fichiers de files ne sont pas écrits sur le disque lorsque la destination est sensible, comme pour des fichiers ou des commndes. Au lieu de cela, les programmes tel que l'agent de livraison local essayent de prendre leurs décisions avec le souci de la sécurité sur la base des informations reçues initialement.

Bien sûr, les programmes Postfix ne font pas confiance au données reçues du réseau. En particulier, Postfix filtre les données fournies par l'utilisateur avant de les exporter via des variables d'environnement. S'il y a une leçon à tirer de ce que les administrateurs ont appris des désastres de la sécurité des sites web, c'est bien ceci : ne laissez jamais des données reçues du réseau approcher de l'interpréteur de commandes. Le filtrage est la meilleure des possibilités possibles.

Données volumineuses

La mémoire pour les chaînes de caractères et les tampons est affectée dynamiquement afin d'éviter tous problèmes de
Les lignes longues dans les messages sont fractionnées en morceaux de taille raisonnable et réassemblées à la livraison
Les diagnostics sont également fractionnés (en un seul endroit !) avant d'être passés au démon syslog afin d'éviter d
Aucun dispositif de défense contre les lignes de commande anormalement longues n'est réalisé, les noyaux Unix impos

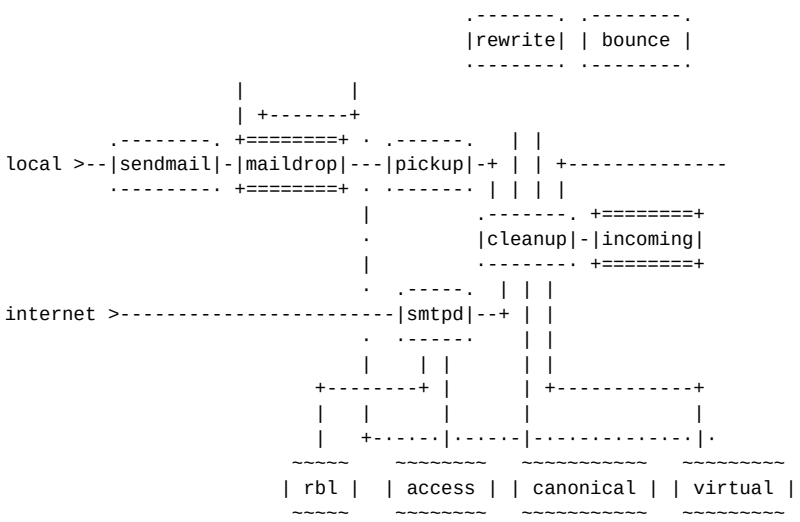
Autres défenses

Le nombre d'instances d'un objet donné en mémoire est limité, afin d'éviter au système de devenir instable en cas de c
En cas de problème, le programme se mettra en veille avant d'envoyer un message d'erreur au client, avant de se plante

Anatomie

Réception du courrier

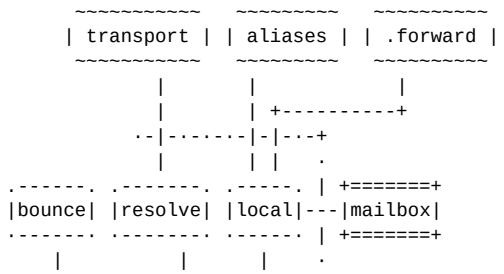
Le premier point d'arrêt à l'intérieur de Postfix d'un message arrivant au système est la file incoming.

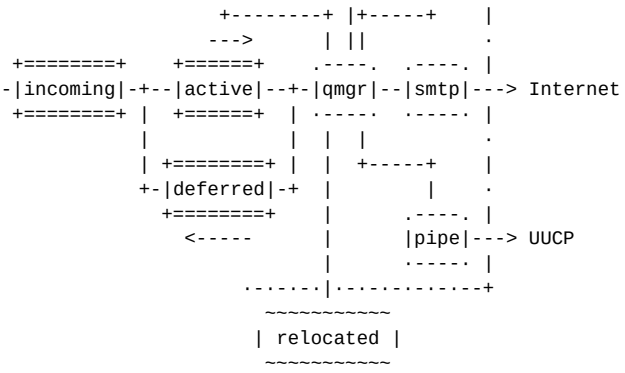


Le message a été posté localement. Le programme sendmail de Postfix le dépose dans le répertoire de la file mai
Le courrier vient du réseau. Le programme smtpd a reçu le message et effectué les tests sanitaires. Le serveur smtp peu
Le courrier a été généré par le système Postfix lui-même, dans le but de renvoyer un message non-délivrable à son
Le courrier a été renvoyé par le démon de livraison local, soit du fait d'une entrée dans la base d'alias, soit à cause d'u
Le courrier a été généré par le système Postfix lui-même, dans le but d'avertir le postmaster d'un problème (chem
Le démon cleanup se charge de la dernière tâche à effectuer sur le courrier entrant. Il ajoute les champs d'e
À la demande du démon cleanup, c'est le démon trivial-rewrite qui réécrit les adresses au standard utilisateu

Livraison du courrier

Une fois le message arrivé dans la file incoming, il reste à le livrer.





- Le gestionnaire de file (`qmgr` : *queue manager*) est le coeur du système de courrier `Postfix`. Il contacte les démons de livraison `local`, `smtp` ou `pipe` et leur envoie une demande de livraison le chemin d'accés au fichier de file, l'adresse de l'expéditeur du message, l'hôte auquel livré le message s'il est distant et une ou plusieurs adresses destination.

  Le gestionnaire de files maintient une file `active` courte ne contenant que quelques messages ouverts pour livraison. La file `active` se comporte comme une fenêtre sur les files `incoming` et `deferred`, éventuellement beaucoup plus larges. Le fait de maintenir la file `active` courte permet de ne pas se trouver à cours de mémoire en cas de charge importante.

  Optionnellement, le gestionnaire de files rejette le courrier dont les destinataires sont listés dans la table `relocated`. Cette table contient les coordonnées pour des utilisateurs ou même des domaines entiers qui n'existent plus.

- À la demande du gestionnaire de files, le démon `trivial-rewrite` résoud les destinations. Par défaut, il ne distingue que deux types de destination : locale ou distante. Des informations complémentaires sur le cheminement du courrier peuvent être spécifiées dans la table optionnelle `transport`.
- À la demande du gestionnaire de files, le démon `bounce or defer` genère des rapports d'impossibilité de livraison quand les courriers ne peuvent pas être livrés, soit à cause d'un erreur irréversible ou bien à cause d'une destination inaccessible pendant une longue période.
- Le démon de livraison `local` connaît le style de boîte `Unix`, la base d'alias à la `Sendmail` et les fichiers `.forward` utilisateurs. Plusieurs agents de livraison `local` peuvent être lancés en parallèle, mais le nombre d'agents lancé pour livrer des messages à un même utilisateur est limité.

  Avec l'agent `sendmail` de `postfix` qui permet de poster des courriers, l'agent de livraison `local` forme l'habituelle interface utilisateur connue avec `Sendmail`.

  L'agent de livraison `local` a quelques fonctionnalités supplémentaires qui permettent d'autres formes de livraison du courrier ; il est possible de le configurer pour livrer les courriers dans les fichiers de boîtes aux lettres dans les répertoires utilisateurs, et il est même possible de déléguer la livraison à une commande extérieure comme le programme procmail bien connu.

- Le client smtp recherche la liste des échangeurs de fichiers du domaine distant, la trie par ordre de préférence et essaye chacune des entrées jusqu'à trouver un serveur qui réponde. Sur les systèmes Postfix particulièrement chargés, plusieurs clients smtp peuvent fonctionner simultanément.
- Le démon pipe est l'interface unique pour tous les autres modes de transport de courrier (en sortie, le programme sendmail étant l'interface d'entrée unique). Le système Postfix est livré avec des exemples de configuration permettant de livrer du courrier via uucp.

Dans les coulisses

Les deux sections précédentes présentaient une vue simplifié du système Postfix. Plusieurs autres choses se passent en arrière-plan, qu'il est difficile de représenter sur un schéma en deux dimensions.

Le démon-maître master est un processus de supervision qui veille au non déroulement des opérations et à la s
La démon bounce or defer peut être appelé par n'importe quel autre démon afin pour chaque message les fichier
Le démon trivial-rewrite peut également être appelé par les autres démons afin de réécrire les adresses au st
Le démon showq l'état de la file Postfix. C'est le programme caché derrière la commande mailq.

Utilitaires en ligne de commande

Assez parlé des démons ! La leçon d'anatomie se termine par une présentation des utilitaires de ligne de commande disponibles pour une utilisation de Postfix au jour le jour. Aux côtés de sendmail, mailq, et newaliases qui ont déjà été présentées, le système Postfix est livré avec une collection d'utilitaires. Pour simplifier, ils sont tous nommés postquelquechose.

La commande postfix contrôle le système. C'est l'interface qui permet de démarrer et d'arrêter le système. E
La commande postalias permet de reconstruire la base d'alias, c'est elle qui est derrière la commande newali
La commande postcat affiche le contenu des fichiers de files. Ce n'est qu'un utilitaire limité, de bas nivea
La commande postconf affiche la configuration du système : valeurs en cours, valeurs par défaut, ou paramètr
La commande postdrop est l'agent qui permet de posetr du courrier, utilisé par la commande sendmail sur les
La commande postkick établit des canaux de communication internes, qui peuvent être mis à disposition de ssc
La commande postlock assure un mécanisme de verrouillage des boîte aux lettres utilisateurs qui et peut être
La commande postlog rend accessible la journalisation de Postfix aux scripts *shell.*
La commande postmap maintient les tables telles que canonical ou [2]virtual.
La commande postuser se charge des files. Elle supprime les fichiers temporaires obsolètes et déplace les fi

Configuration

Configuration de base

Introduction

Postfix a près de 100 paramètres controllés via le fichier main.cf. Heureusement, ces paramètres ont des valeurs par défaut plutôt appropriées. Dans la plupart des cas, seuls deux ou trois d'entre eux doivent être configurés pour rendre Postfix utilisables.

Quel domaine utiliser pour le courrier sortant ?
Pour quels domaines recevoir du courrier ?

Les valeurs par défaut de nombreux autres paramètres découlent de ces deux-là.

Le troisième paramètre sensible contrôle le niveau et donc le nombre des alertes envoyées aux postmaster :

Quels problèmes rapporter au postmaster ?

Lorsque des paramètres ont été changés dans les fichiers de configuration de Postfix, la commande postfix reload permet de charger la nouvelle configuration.

Si Postfix utilise une interface réseau virtuelle, ou bien si le système héberge d'autres systèmes postfix sur des interfaces virtuelles, les paramètres suivants devront être règlés également.

Mon propre nom d'hôte
Mon propre nom de domaine
Mes propres réseaux
Mes propres adresses réseau

Quel domaine utiliser pour le courrier sortant ?

Le paramètre myorigin indique le domaine qui apparaîtra sur tout courrier posté localement. La valeur par défaut est le paramètre $myhostname dont la valeur par défaut est le nom de la machine. À moins de ne travailler que sur un très petit domaine, la valeur du paramètre $mydomain dont la valeur par défaut est le nom de domaine de la machine peut être préférable.

Pour quels domaines recevoir le courrier ?

Le paramètre mydestination indique pour quels domaines cette machine va délivrer le courrier localement au lieu de le faire suivre à une autre machine. La valeur par défaut permet de recevoir le courrier pour la machine elle-même et seulement.

Il est possible de préciser aucun, un ou plusieurs noms de domaine, directement, par l'inclusion de fichiers /chemin/fichier ou la lecture de tables type :nom en séparant les différentes entrées par des espaces ou des virgules. La table virtual est destinée à contenir ce genre d'informations.

Si votre machine est un serveur pour tout votre domaine, il faut y faire figurer `$mydomain`.

Afin d'éviter les boucles de routage du courrier, il faut lister tous les noms de la machine, y compris `localhost.$localdomain` et `$myhostname`.

Quels problèmes rapporter au `postmaster` ?

Il est d'abord nécessaire de mettre en place un alias associant le `postmaster` à une personne réelle.

Les utilisateurs peuvent utiliser cette adresse, mais le système `Postfix` lui-même l'utilisera pour rapporter d'éventuels problèmes. Tous les types de problèmes pouvant être rapportés ne sont pas forcément intéressants, c'est pourquoi ce mécanisme est configurable. La valeur par défaut indique de ne rapporter au `postmaster` que les problèmes sérieux (ressources, logiciel).

C'est le paramètre `notify_classes` qu'il convient de règler. Les significations des différentes classes de rapport sont les suivantes :

`bounce`

: une copie des messages non-délivrables est envoyée au `postmaster`. Le massage d'alerte qui accompagne le copie du message original est appelée `bounce`. Pour des raisons de confidentialité, la copie est amputée après l'entête.

`bounce2`

: deux messages de bounce sont envoyés au `postmaster`.

`delay`

: le `postmaster` est informé de tout message dont la livraison a été retardée.

`policy`

: le `postmaster` est alerté en cas de violation des contrôles uce, une transcription complète de la session smtp étant jointe au message.

`protocol`

: le `postmaster` est informé des erreurs de protocole et des tentatives de commandes utilisateur inexistantes. Là-aussi, une transcription complète de la session smtp est jointe au message.

`resource`

: le `postmaster` est informé des non-livraisons de courrier liées à des problèmes de ressources.

`software`

: le `postmaster` est informé des non-livraisons de courrier liées à des problèmes logiciels.

Mon propre nom d'hôte

Le paramètre myhostname indique le nom complet et conforme de la machine sur laquelle fonctionne le système Postfix. La valeur $myhostname apparaît dans la valeur par défaut de nombreux paramètres de configuration de Postfix.

Par défaut, le paramètre myhostname a pour valeur le nom de la machine. Si le nom de la machine n'st pas le nom complet et conforme, ou si le système Postfix fonctionne sur une interface virtuelle, il est nécessaire de spécifier ici le nom à utiliser.

Mon propre nom de domaine

Le paramètre mydomain spécifie quelle est la partie domaine de $myhostname. Par défaut, la valeur de ce paramètre est issue de $myhostname : le premier terme étant supprimé.

Mes propres réseaux

Ce paramètre permet de spécifier les réseaux à considérer comme locaux. La valeur est utilisée par les contrôles uce.

Par défaut, $mynetworks est le réseau de classe A, B ou C auquel est attachée l'interface réseau.

Mes propres adresses réseau

Le paramètre inet_interfaces permet e spécifier au système sur quelles adresses réseau il devra écouter ; tout courrier envoyé à utilisateur@adresse.ip sera délivré localement comme s'il était adressé à l'un des domaines listés par $mydestination.

Par défaut, le système écoute sur toutes les interfaces. Ce paramètre permet de faire fonctionner plusieurs systèmes Postfix sur la même machine, chacun utilisant une interface réseau virtuelle différente. Si un système Postfix concerne le courrier pour la machine elle-même, sa configuration devra interdire l'écoute des interfaces virtuelles, cette situation pouvant causer des boucles de routage du courrier.

Contrôles uce

Postfix offre une variété de paramètres qui permettent de limiter la distribution de courrier commercial non sollicité (uce : *unsollicited commercial e-mail*).

Par défaut, le serveur smtp du système Postfix n'acceptera le courrier que s'il provient d'un réseau considéré comme local, ou s'il est adressé à l'un des domaines hébergés par le système. Votre système ne pourra donc pas être utilisé comme un relais pour les courriers indésirables d'étrangers non-identifiés.

Le texte de cette section explique comment mettre en oeuvre une politique anti-uce plus pointue, par la mise en oeuvre de liste d'accés à-la Sendmail et/ou de l'utilisation de serveurs de noms rbl (*real-time blackhole list, ou reject black list*).

Sauf exception dûment indiquée, les paramètres suivants sont dans le fichier main.cf.

Filtrage des entêtes

Le paramètre `header_checks` restreint les données autorisées dans l'entête des messages. Par défaut, tout est autorisé. La valeur du paramètre doit pointé une ou plusieurs tables décrivant des entêtes interdits.

Restrictions sur le nom d'hôte et l'adresse ip des clients

Le paramètre `smtpd_client_restrictions` permet de restreindre les clients pour lesquels le serveur acceptera des connexions. Par défaut, toutes les connexions sont acceptées. Il existe septs restrictions prédéfinies listées ci-dessous. La valeur du paramètre peut aussi pointer une ou plusieurs tables.

`reject_unknown_client`

Si la résolution de nom du client est impossible, le courrier est rejeté. Le paramètre `unknown_client_reject_code` spécifie le code réponse que le serveur fournira au client (`450` par défaut).

`permit_mynetworks`

Autorise toutes les requêtes issues d'une machine d'un réseau listés par `$mynetworks`.

`check_client_access type:nom`

ce paramètre recherche dans la table d'accés indiquée le nom d'hôte, de domaine, l'adresse ip, ou de réseau à la recherche d'une directive `REJECT`, `OK` ou `RELAY`. Le paramètre `access_map_reject_code` spécifie le code réponse que le serveur fournira au client (`554` par défaut).

`reject_maps_rbl`

La requête est rejetée si l'adresse réseau du client est listée dans `$maps_rbl_domains`. La paramêtre `maps_rbl_reject_code` spécifie le code réponse (`554` par défaut).

permit, reject et reject_unauth_pipelining

voir « Restrictions générales ».

Commande `HELO` (`EHLO`) requise

Le paramètre smtpd_helo_required permet de rendre obligatoire la commande helo au début de la session smtp. Le fait de requérir cette commande bloque certains logiciels uce. Par défaut, la commande n'est pas requise. La valeur peut être *yes* ou *no*>.

Restriction sur le nom d'hôte fourni par la commande HELO (EHLO)

La paramètre smtpd_helo_restrictions permet de contrôler la vérification des données fournies par la commande HELO (EHLO). Par défaut, aucune analyse des données n'est effectuée. Il existe cinqs restrictions spécifiques prédéfinies listées ci-dessous, mais les septs restrictions applicables au nom d'hôte et à l'adresse ip des clients peuvent aussi être utilisées.

reject_invalid_hostname

rejète la requête si la syntaxe du nom d'hôte normalement fourni par la commande HELO est invalide. Le paramètre invalid_hostname_reject_code spécifie le code réponse que le serveur fournira au client (501 par défaut).

permit_naked_ip_address

autorise la commande HELO à envoyer l'adresse ip nue, sans les crochets [] spécifiés par la rfc. Maheureusement, de nombreux logiciels clientsde courrier électroniques procède de cette façon.

reject_unknown_hostname

rejète la requête si la résolution inverse sur le nom fourni par la commande HELO est impossible. Le paramètre unknown_hostname_reject_code spécifie le code réponse que le serveur fournira au client (450 par défaut).

reject_non_fqdn_hostname

rejète la requête si le nom fourni par la commande HELO n'est pas complet et conforme. Le paramètre non_fqdn_reject_code spécifie le code réponse que le serveur fournira au client (504 par défaut).

check_helo_access type:nom

ce paramètre recherche dans la table d'accés indiquée le nom d'hôte, de domaine, l'adresse ip, ou de réseau à la recherche d'une directive REJECT, OK ou RELAY. Le paramètre access_map_reject_code spécifie le code réponse que le serveur fournira au client (554 par défaut).

Stricte conformité de l'adresse de l'enveloppe à la rfc821 requise

Le paramètre strict_rfc821_envelopes permet de contrôler le niveau de tolérance de Postfix sur la conformité des adresses fournies par les commandes MAIL FROM et RCPT TO. Malheureusement, Sendmail est laxiste à ce sujet et de nombreux logiciels clients de courrier pensent s'en sortir sans

respecter les standards. Être strict bloquera non seulement des courriers indésirables, mais aussi certains courriers légitimes envoyés avec les logiciels client mal conçus.

Par défaut, le serveur smtp de Postfix accepte toutes les adresses auxquelles il peut trouver un sens, en particulier les adresses conformes à la rfc822 et les adresses non encadrées de <>. Il y a beaucoup de clients aussi mal conçus utilisés sur l'*Internet*.

Restrictions sur l'adresse de l'expéditeur

Le paramètre smtpd_sender_restrictions permet de restreindre les messages acceptés pour livraison en fonction de la valeur donnée par la commande MAIL FROM. Par défaut, Postfix accepte les courriers quelle que soit cette valeur.

Il existe trois restrictions spécifiques prédéfinies et listées ci-dessous, mais les douzes restrictions applicables aux clients et à la valeur fournie par la commande HELO peuvent aussi être utilisées.

reject_unknown_sender_domain

La requête est rejetée si l'adresse fournie n'a pas de correspondance mx ou dns. Le paramètre unknown_address_reject_code permet de préciser le code d'erreur fourni au client (450 par défaut). Le code sera 450 si l'erreur est dûe à une erreur dns temporaire.

check_sender_access type:nom

ce paramètre recherche dans la table d'accés indiquée le nom d'hôte, de domaine, l'adresse ip, ou de réseau à la recherche d'une directive REJECT, OK ou RELAY. Le paramètre access_map_reject_code spécifie le code réponse que le serveur fournira au client (554 par défaut).

reject_non_fqdn_sender

la requête est rejetée si l'adresse fournie n'est pas complète et conforme. Le paramètre non_fqdn_reject_code permet de préciser le code d'erreur fourni au client (504 par défaut).

Restrictions sur l'adresse du destinataire

Le paramètre smtpd_sender_restrictions permet de restreindre les adresses expéditeur, fournies par la commande MAIL FROM, ayant droit d'envoyer du courrier.

Restrictions de la commande ETRN

Restrictions générales

Paramètres de contrôle uce supplémentaires

Contrôles des taux

Contrôles des ressources

Manipulation des adresses

Introduction

Bien que le système Postfix ne comprenne pas encore de langage de réécriture digne de ce nom, il est capable d'effectuer quelques manipulations des adresses en utilisant des requêtes sur des tables. Lorsqu'un message traverse le système Postfix, ses adresses sont modifiées dans l'ordre décrit ci-dessous.

Pour n'importe quel courrier :

Réécriture des adresses au format standard
Correspondance avec des adresses canoniques
Masquage d'adresses
Correspondance avec des adresses virtuelles
Table des utilisateurs déplacés
Sélection du mode de transport

Pour les courriers locaux :

Base d'alias
Fichiers .forward utilisateurs
Utilisateurs inexistants

Réécriture des adresses au format standard

Le démon cleanup, avant de vérifier la correspondance d'une adresse avec les tables, commence par réécrire cette adresse au format standard utilisateur@domaine.complet.et.conforme en passant cette adresse au démon trivial-rewrite. L'objectif de la réécriture au format standard est de réduire le nombre d'entrées nécessaires dans les tables.

Le démon trivial-rewrite implémente les schémas de réécriture suivants :

`@hotea,@hoteb:utilisateur@site` vers `utilisateur@site`

La fonctionnalité de routage à la source est obsolète. `Postfix` n'implémente pas cette fonctionnalité et doit donc supprimer la route indiquée.

`site!user` vers `user@site`

Cette fonctionnalité est controllée par le paramètre booléen `swap_bangpath` (activé par défaut : *yes*). L'objectif est réécrire les adresses uucp dans le style domaine. Cette réécriture est utile pour les sites recevant du courrier via uucp, mais elle n'apportera aucun problèmes aux autres.

`user%domain` vers `user@domain`

Cette fonctionnalité est controllé par le paramètre `allow_percent_hack`. Généralement, elle est utilisée pour gérer les adresses du type `user%domaine@autre_domaine`.

`user` vers `user@$myorigin`

Cette fonctionnalité est controllée par le paramètre `append_at_myorigin`. L'objectif est d'haromoniser le traitement des courriers utilisateur des machines du domaine `$myorigin`.

Il est déconseillé de désactiver cette fonctionalité, `Postfix` attendant les adresses sous la forme `user@domain`.

Si le système `Postfix` n'est pas le serveur principal pour le domaine `$myorigin`, et que le courrier de certains utilisateurs doit être livré en local, il faut créer une entrée dans la table `virtual` redirigeant `utilisateur@$myorigin` vers `utilisateur@$myhostname`.

`utilisateur@hote` vers `utilisateur@hote.$mydomain`

Cette fonctionnalité est controllée par le paramètre `append_dot_mydomain` (activé par défaut : *yes*). L'objectif est de traiter de la même façon plusieurs formes de nommage d'un même hôte.

Certains jugent la réécriture de `hote` vers `hote.$mydomain` néfaste. C'est pourquoi il est possible de désactiver cette fonctionnalité. D'autres apprécient de voir le domaine ajouté automatiuement.

`utilisateur@site.` vers `utilisateur@site` (sans le point final).

Correspondance avec des adresses canoniques

Avant de déposer les messages dans la file `incoming`, le démon `cleanup` utilise la table `canonical` pour réécrire toutes les adresses de l'enveloppe et de l'entête. Cette correspondance est utile pour remplacer des nom de *login* utilisateurs par des adresses du style `Prenom.Nom`, ou pour supprimer des noms de domaine invalides éventuellement ajoutés par des systèmes de courrier illicites.

La correspondancen canonique est désactivée par défaut. Pour l'activer, il faut éditer le paramètre `canonical_maps` dans le fichier de configuration `main.cf` et lui spécifier une ou plusieurs tables.

En plus des tables `canonical` qui s'appliquent à la fois aux adresses expéditeur et destinataire, il est possible de déclarer des tables canoniques qui s'appliquent aux adresses expéditeur ou destinataires, respectivement avec les paramètres `sender_canonical_maps` et `recipient_canonical_maps`.

Ces tables sont lues avant la table commune.

La réécriture des adresses expéditeur est utile pour transformer des adresses laides en une forme plus agréable, tout en permettant d'écrire aux vilaines adresses sans créer de boucle de routage du courrier.

Masquage d'adresses

Le masquage d'adresses consiste à cacher tous les hôtes d'un domaine derrière une passrelle de courrier, et à faire apparaître le courrier comme provenant de la passerelle elle-même, au lieu de machines individuelles.

Le masquage d'adresses est désactivé par défaut. Pour l'activer, il faut éditer le paramètre `masquerade_domains` dans le fichier `main.cf` et y spécifier un ou plusieurs domaines.

Le paramètre `masquerade_exceptions` indique quels noms d'utilisateur ne doivent pas être soumis au masquage d'adresses.

Par défaut, `Postfix` ne fait aucune exception.

Attention, subtilité : le masquage d'adresses ne s'applique qu'aux adresses de l'entête et à l'adresse expéditeur de l'enveloppe, et pas à l'adresse destinataire de l'enveloppe.

Correspondance avec des adresses virtuelles

Après avoir appliqué les correspondances canoniques et de masquage, le démon `cleanup` utilise la table `virtual` pour rediriger le courrier vers les différents destinataires locaux ou distants. Seules l'adresse destinataire de l'enveloppe est affectée par cette correspondance. Les correspondances par recherche dans la table virtual sont utiles pour rediriger le courrier à des domaines virtuels dans des boîtes d'utilisateur réel, et pour rediriger le courrier adressé à des utilisateurs qui n'existent plus. Les requêtes sur la table virtual peuvent aussi permettre la transformation Prenom.Nom en nom de login utilisateur réel, bien que la base d'alias local semble être plus appropriée.

La rcherche de correspondance dans les tables virtual est déasactivée par défaut. Pour l'activer, il faut affecter au paramètre `virtual_maps`, une valeur pointant une ou plusieurs tables.

Les adresses trouvées dans les tables `virtual` sont peuvent être sujettes à une autre recherche de correspondance dans les tables `virtual`, mais elles ne passeront pas la recherche de correspondance `canonical`, afin d'éviter des boucles de routage de courrier.

Table des utilisateurs déplacés

L'étape suivante dans la réécriture des adresses est réalisée par le gestionnaire de files qui vérifie la corrspondance de chaque adresse destinataire avec la table `relocated`. Cette table fournit les informations nécessaires pour atteindre les utilisateurs qui n'ont plus de compte et pour gérer les domaines qui n'existent plus. Lorsqu'un message est envoyé à l'une des adresses comprises dans cette table, il est renvoyé avec un message d'information à son expéditeur.

Les recherches d'utilisateurs déplacés sont désactivées par défaut. Pour les activer, il faut affecter une valeur de table au paramètre `relocated_maps`.

Sélection du mode de transport

Une fois que le gestionnaire de files a établit la destination, la table `transport`, optionnelle, contrôle le mode de transport (elle est utilisée par le démon `trivial-rewrite`). Par défaut, tout est délivré par smtp. La table de transport peut être utilisée pour envoyer le courrier de certains sites via uucp, ou pour gérer l'envoi de courrier à des sites qui ne peuvent assurer qu'une connexion smtp à la fois.

Par défaut, cette fonctionnalité est désactivée. C'est le paramètre `transport_maps` dont la valeur doit indiquer une table au moins qui permet son activation.

Base d'alias

Quand le courrier doit être délivré localement, le démon `local` vérifie la concordance de chaque destinataire avec les entrées de la base d'alias. La recherche de correspondance n'affecte pas les adresses de l'entête. Généralement, les alias locaux sont utilisés pour créer des listes de diffusion ou pour rediriger des alias standards comme `postmaster` vers des utilisateurs réels. La base peut aussi être utilisée pour faire correspondre une adresse du type `Prenom.Nom` à un login utilisateur.

La base d'alias est activée par défaut. Le chemin d'accés à la base configurée par défaut dépend du système d'exploitation.

Pour des raisons de sécurité, les livraisons de courrier à des commandes ou des fichiers sont effectuées avec les droits du propriétaire de la base. L'identifiant utilisateur correspondant au paramètre `default_privs` est utilisé pour les bases appartenant à *root*.

Fichiers `.forward` utilisateurs

Les utilisateurs ont la possibilité de contrôler la livraison de leur propre courrier en indiquant la redirection de celui-ci dans le fichier `.forward` placé dans leur répertoire personnel. La syntaxe de ces fichiers est la même que celle du fichier d'alias.

Utilisateurs inexistants

Lorsque le démon de livraison s'aperçoit qu'un utilisateur est inexistant, le message est renvoyé à l'expéditeur (« utilisateur inconnu »). Parfois, il peut être souhaitable de faire suivre le courrier pour des utilisateurs inexistants à une autre machine. Dans cet esprit, il est possible de spécifier une destination alternative au paramètre `luser_relay`.

Alternativement, il est possible de déléguer à un autre mode de transport le courrier destiné à des utilisateurs inexistants en affectant judicieusement le paramètre fallback_transport.

FAQ

Annexe A.

ce document est disponible :

- en ligne : http://linux.crdp.ac-caen.fr/postfix/
- au format xml, fichier source, dtd *docbook-xml* version 3.1.3 : http://linux.crdp.ac-caen.fr/postfix/postfix.xml
- au format pdf : http://linux.crdp.ac-caen.fr/postfix/postfix.pdf