Red Hat Enterprise Linux 9

Déploiement de serveurs de messagerie

Configuration et maintenance des services de serveur de messagerie

Last Updated: 2023-06-14

Red Hat Enterprise Linux 9 Déploiement de serveurs de messagerie

Configuration et maintenance des services de serveur de messagerie

Notice légale

Résumé

Sur Red Hat Enterprise Linux, vous pouvez fournir des services de messagerie fiables et sécurisés à vos clients et utilisateurs internes en utilisant l'agent de transport de messagerie Postfix comme service SMTP et l'agent de distribution de messagerie Dovecot comme services IMAP et POP3. Ces deux services s'intègrent l'un à l'autre et prennent en charge les backends centraux, tels que les annuaires LDAP pour stocker les données de compte et authentifier les utilisateurs.

Table des matières

RENDRE L'OPEN SOURCE PLUS INCLUSIF

Red Hat s'engage à remplacer les termes problématiques dans son code, sa documentation et ses propriétés Web. Nous commençons par ces quatre termes : master, slave, blacklist et whitelist. En raison de l'ampleur de cette entreprise, ces changements seront mis en œuvre progressivement au cours de plusieurs versions à venir. Pour plus de détails, voir le message de notre directeur technique Chris Wright.

FOURNIR UN RETOUR D'INFORMATION SUR LA DOCUMENTATION DE RED HAT

Nous apprécions vos commentaires sur notre documentation. Faites-nous savoir comment nous pouvons l'améliorer.

Soumettre des commentaires sur des passages spécifiques

1. Consultez la documentation au format **Multi-page HTML** et assurez-vous que le bouton **Feedback** apparaît dans le coin supérieur droit après le chargement complet de la page.
2. Utilisez votre curseur pour mettre en évidence la partie du texte que vous souhaitez commenter.
3. Cliquez sur le bouton **Add Feedback** qui apparaît près du texte en surbrillance.
4. Ajoutez vos commentaires et cliquez sur **Submit**.

Soumettre des commentaires via Bugzilla (compte requis)

1. Connectez-vous au site Web de Bugzilla.
2. Sélectionnez la version correcte dans le menu **Version**.
3. Saisissez un titre descriptif dans le champ **Summary**.
4. Saisissez votre suggestion d'amélioration dans le champ **Description**. Incluez des liens vers les parties pertinentes de la documentation.
5. Cliquez sur **Submit Bug**.

CHAPITRE 1. CONFIGURATION ET MAINTENANCE D'UN SERVEUR DOVECOT IMAP ET POP3

Dovecot est un agent de distribution de courrier électronique (MDA) très performant qui met l'accent sur la sécurité. Vous pouvez utiliser des clients de messagerie compatibles IMAP ou POP3 pour vous connecter à un serveur Dovecot et lire ou télécharger des messages électroniques.

Caractéristiques principales de Dovecot :

- La conception et la mise en œuvre sont axées sur la sécurité
- Prise en charge de la réplication bidirectionnelle pour la haute disponibilité afin d'améliorer les performances dans les grands environnements
- Prend en charge le format de boîte aux lettres haute performance **dbox**, mais aussi **mbox** et **Maildir** pour des raisons de compatibilité
- Fonctionnalités d'autoréparation, telles que la correction des fichiers d'index cassés
- Respect des normes IMAP
- Prise en charge des solutions de contournement des bogues dans les clients IMAP et POP3

1.1. MISE EN PLACE D'UN SERVEUR DOVECOT AVEC AUTHENTIFICATION PAM

Dovecot supporte l'interface Name Service Switch (NSS) comme base de données utilisateurs et le framework Pluggable Authentication Modules (PAM) comme backend d'authentification. Avec cette configuration, Dovecot peut fournir des services aux utilisateurs qui sont disponibles localement sur le serveur à travers NSS.

Utiliser l'authentification PAM pour les comptes :

- Ils sont définis localement dans le fichier **/etc/passwd**
- Sont stockés dans une base de données distante, mais ils sont disponibles localement par l'intermédiaire du System Security Services Daemon (SSSD) ou d'autres plugins NSS.

1.1.1. Installation de Dovecot

Le paquet **dovecot** fournit :

- Le service **dovecot** et les services publics pour le maintenir
- Les services que Dovecot démarre à la demande, par exemple pour l'authentification
- Plugins, tels que le filtrage du courrier côté serveur
- Fichiers de configuration dans le répertoire **/etc/dovecot/**
- Documentation dans le répertoire **/usr/share/doc/dovecot/**

Procédure

- Installez le paquetage **dovecot**:

```
# dnf install dovecot
```

NOTE

Si Dovecot est déjà installé et que vous avez besoin de fichiers de configuration propres, renommez ou supprimez le répertoire **/etc/dovecot/**. Ensuite, réinstallez le paquetage. Sans supprimer les fichiers de configuration, la commande **dnf reinstall dovecot** ne réinitialise pas les fichiers de configuration dans **/etc/dovecot/**.

Prochaine étape

- Configuration du cryptage TLS sur un serveur Dovecot .

1.1.2. Configuration du cryptage TLS sur un serveur Dovecot

Dovecot fournit une configuration sécurisée par défaut. Par exemple, TLS est activé par défaut pour transmettre des informations d'identification et des données cryptées sur les réseaux. Pour configurer TLS sur un serveur Dovecot, il suffit de définir les chemins d'accès aux fichiers de certificats et de clés privées. De plus, vous pouvez augmenter la sécurité des connexions TLS en générant et en utilisant les paramètres Diffie-Hellman pour fournir un secret parfait (PFS).

Conditions préalables

- Dovecot est installé.
- Les fichiers suivants ont été copiés aux emplacements indiqués sur le serveur :
  - Le certificat du serveur : **/etc/pki/dovecot/certs/server.example.com.crt**
  - La clé privée : **/etc/pki/dovecot/private/server.example.com.key**
  - Le certificat de l'autorité de certification (CA) : **/etc/pki/dovecot/certs/ca.crt**
- Le nom d'hôte figurant dans le champ **Subject DN** du certificat du serveur correspond au nom de domaine complet (FQDN) du serveur.

Procédure

1. Définir des autorisations sécurisées pour le fichier de la clé privée :

```
# chown root:root /etc/pki/dovecot/private/server.example.com.key
# chmod 600 /etc/pki/dovecot/private/server.example.com.key
```

2. Générer un fichier avec les paramètres Diffie-Hellman :

```
# openssl dhparam -out /etc/dovecot/dh.pem 4096
```

   En fonction du matériel et de l'entropie du serveur, la génération de paramètres Diffie-Hellman avec 4096 bits peut prendre plusieurs minutes.

3. Définissez les chemins d'accès aux fichiers de certificats et de clés privées dans le fichier **/etc/dovecot/conf.d/10-ssl.conf**:

   a. Mettez à jour les paramètres **ssl_cert** et **ssl_key** et définissez-les de manière à utiliser les

a. Mettez à jour les paramètres **ssl_cert** et **ssl_key** et définissez-les de manière à utiliser les chemins d'accès au certificat et à la clé privée du serveur :

```
ssl_cert = </etc/pki/dovecot/certs/server.example.com.crt
ssl_key = </etc/pki/dovecot/private/server.example.com.key
```

b. Décommentez le paramètre **ssl_ca** et définissez-le de manière à utiliser le chemin d'accès au certificat d'autorité de certification :

```
ssl_ca = </etc/pki/dovecot/certs/ca.crt
```

c. Décommentez le paramètre **ssl_dh** et indiquez-lui le chemin d'accès au fichier des paramètres Diffie-Hellman :

```
ssl_dh = </etc/dovecot/dh.pem
```

IMPORTANT

Pour s'assurer que Dovecot lit la valeur d'un paramètre à partir d'un fichier, le chemin d'accès doit commencer par le caractère **<**.

Prochaine étape

- Préparer Dovecot à utiliser des utilisateurs virtuels

Ressources supplémentaires

- **/usr/share/doc/dovecot/wiki/SSL.DovecotConfiguration.txt**

1.1.3. Préparer Dovecot à utiliser des utilisateurs virtuels

Par défaut, Dovecot effectue de nombreuses actions sur le système de fichiers en tant qu'utilisateur du service. Cependant, configurer le back-end de Dovecot pour qu'il utilise un utilisateur local pour effectuer ces actions présente plusieurs avantages :

- Dovecot effectue des actions sur le système de fichiers en tant qu'utilisateur local spécifique au lieu d'utiliser l'ID de l'utilisateur (UID).
- Les utilisateurs n'ont pas besoin d'être disponibles localement sur le serveur.
- Vous pouvez stocker toutes les boîtes aux lettres et tous les fichiers spécifiques à l'utilisateur dans un répertoire racine.
- Les utilisateurs n'ont pas besoin d'un UID et d'un GID, ce qui réduit les efforts d'administration.
- Les utilisateurs qui ont accès au système de fichiers du serveur ne peuvent pas compromettre leurs boîtes aux lettres ou leurs index, car ils ne peuvent pas accéder à ces fichiers.
- La mise en place de la réplication est plus facile.

Conditions préalables

- Dovecot est installé.

Procédure

1. Créez l'utilisateur **vmail**:

```
# useradd --home-dir /var/mail/ --shell /usr/sbin/nologin vmail
```

   Dovecot utilisera par la suite cet utilisateur pour gérer les boîtes aux lettres. Pour des raisons de sécurité, n'utilisez pas les utilisateurs du système **dovecot** ou **dovenull** à cette fin.

2. Si vous utilisez un chemin différent de celui de **/var/mail/**, définissez le contexte SELinux de **mail_spool_t**, par exemple :

```
# semanage fcontext -a -t mail_spool_t "<path>(/.*)?"
# restorecon -Rv <path>
```

3. Accordez les droits d'écriture sur **/var/mail/** uniquement à l'utilisateur **vmail**:

```
# chown vmail:vmail /var/mail/
# chmod 700 /var/mail/
```

4. Décommentez le paramètre **mail_location** dans le fichier **/etc/dovecot/conf.d/10-mail.conf** et attribuez-lui le format et l'emplacement de la boîte aux lettres :

```
mail_location = sdbox:/var/mail/%n/
```

   Avec ce réglage :

   - Dovecot utilise le format de boîte aux lettres **dbox** en mode **single**. Dans ce mode, le service stocke chaque courrier dans un fichier séparé, comme dans le format **maildir**.
   - Dovecot résout la variable **%n** dans le chemin du nom d'utilisateur. Ceci est nécessaire pour s'assurer que chaque utilisateur dispose d'un répertoire séparé pour sa boîte aux lettres.

Prochaine étape

- Utilisation de PAM comme backend d'authentification pour Dovecot .

Ressources supplémentaires

- **/usr/share/doc/dovecot/wiki/VirtualUsers.txt**
- **/usr/share/doc/dovecot/wiki/MailLocation.txt**
- **/usr/share/doc/dovecot/wiki/MailboxFormat.dbox.txt**
- **/usr/share/doc/dovecot/wiki/Variables.txt**

1.1.4. Utilisation de PAM comme backend d'authentification pour Dovecot

Par défaut, Dovecot utilise l'interface Name Service Switch (NSS) comme base de données utilisateurs et le framework Pluggable Authentication Modules (PAM) comme backend d'authentification.

Personnalisez les paramètres pour adapter Dovecot à votre environnement et pour simplifier l'administration en utilisant la fonctionnalité des utilisateurs virtuels.

Conditions préalables

- Dovecot est installé.
- La fonctionnalité des utilisateurs virtuels est configurée.

Procédure

1. Mettre à jour le paramètre **first_valid_uid** dans le fichier **/etc/dovecot/conf.d/10-mail.conf** pour définir l'ID utilisateur (UID) le plus bas qui peut s'authentifier à Dovecot :

   ```
   premier_uid_valide = 1000
   ```

   Par défaut, les utilisateurs ayant un UID supérieur ou égal à **1000** peuvent s'authentifier. Si nécessaire, vous pouvez également définir le paramètre **last_valid_uid** pour définir l'UID le plus élevé que Dovecot autorise pour se connecter.

2. Dans le fichier **/etc/dovecot/conf.d/auth-system.conf.ext**, ajoutez le paramètre **override_fields** à la section **userdb** comme suit :

   ```
   userdb {
     driver = passwd
     override_fields = uid=vmail gid=vmail home=/var/mail/%n/
   }
   ```

   En raison des valeurs fixes, Dovecot n'interroge pas ces paramètres à partir du fichier **/etc/passwd**. Par conséquent, le répertoire personnel défini dans **/etc/passwd** n'a pas besoin d'exister.

Prochaine étape

- Terminez la configuration de Dovecot .

Ressources supplémentaires

- **/usr/share/doc/dovecot/wiki/PasswordDatabase.PAM.txt**
- **/usr/share/doc/dovecot/wiki/VirtualUsers.Home.txt**

1.1.5. Compléter la configuration de Dovecot

Une fois que vous avez installé et configuré Dovecot, ouvrez les ports requis dans le service **firewalld**, puis activez et démarrez le service. Vous pouvez ensuite tester le serveur.

Conditions préalables

- Les éléments suivants ont été configurés dans Dovecot :
  - Cryptage TLS
  - Un backend d'authentification
- Les clients font confiance au certificat de l'autorité de certification (AC).

Procédure

1. Si vous souhaitez fournir uniquement un service IMAP ou POP3 aux utilisateurs, décommentez le paramètre **protocols** dans le fichier **/etc/dovecot/dovecot.conf** et définissez-le en fonction des protocoles requis. Par exemple, si vous n'avez pas besoin de POP3, définissez :

```
protocols = imap lmtp
```

   Par défaut, les protocoles **imap**, **pop3** et **lmtp** sont activés.

2. Ouvrez les ports dans le pare-feu local. Par exemple, pour ouvrir les ports des protocoles IMAPS, IMAP, POP3S et POP3, entrez :

```
# firewall-cmd --permanent --add-service=imaps --add-service=imap --add-service=pop3s --add-service=pop3
# firewall-cmd --reload
```

3. Activez et démarrez le service **dovecot**:

```
# systemctl enable --now dovecot
```

Vérification

1. Utilisez un client de messagerie, tel que Mozilla Thunderbird, pour vous connecter à Dovecot et lire les courriels. Les paramètres du client de messagerie dépendent du protocole que vous souhaitez utiliser :

   Tableau 1.1. Paramètres de connexion au serveur Dovecot

Protocol	Port	Sécurité des connexions	Méthode d'authentification
IMAP	143	STARTTLS	PLAIN[a]
IMAPS	993	SSL/TLS	PLAIN[a]
POP3	110	STARTTLS	PLAIN[a]
POP3S	995	SSL/TLS	PLAIN[a]

[a] Le client transmet des données cryptées via la connexion TLS. Par conséquent, les informations d'identification ne sont pas divulguées.

   Notez que ce tableau ne liste pas les paramètres pour les connexions non chiffrées car, par défaut, Dovecot n'accepte pas l'authentification en texte clair sur les connexions sans TLS.

2. Afficher les paramètres de configuration avec des valeurs autres que celles par défaut :

```
# doveconf -n
```

Ressources supplémentaires

- **firewall-cmd(1)** page de manuel

1.2. MISE EN PLACE D'UN SERVEUR DOVECOT AVEC AUTHENTIFICATION LDAP

Si votre infrastructure utilise un serveur LDAP pour stocker les comptes, vous pouvez authentifier les utilisateurs de Dovecot sur ce serveur. Dans ce cas, vous gérez les comptes de manière centralisée dans l'annuaire et les utilisateurs n'ont pas besoin d'un accès local au système de fichiers du serveur Dovecot.

Les comptes gérés de manière centralisée sont également un avantage si vous envisagez de mettre en place plusieurs serveurs Dovecot avec réplication afin de rendre vos boîtes aux lettres hautement disponibles.

1.2.1. Installation de Dovecot

Le paquet **dovecot** fournit :

- Le service **dovecot** et les services publics pour le maintenir
- Les services que Dovecot démarre à la demande, par exemple pour l'authentification
- Plugins, tels que le filtrage du courrier côté serveur
- Fichiers de configuration dans le répertoire **/etc/dovecot/**
- Documentation dans le répertoire **/usr/share/doc/dovecot/**

Procédure

- Installez le paquetage **dovecot**:

```
# dnf install dovecot
```

NOTE

Si Dovecot est déjà installé et que vous avez besoin de fichiers de configuration propres, renommez ou supprimez le répertoire **/etc/dovecot/**. Ensuite, réinstallez le paquetage. Sans supprimer les fichiers de configuration, la commande **dnf reinstall dovecot** ne réinitialise pas les fichiers de configuration dans **/etc/dovecot/**.

Prochaine étape

- Configuration du cryptage TLS sur un serveur Dovecot .

1.2.2. Configuration du cryptage TLS sur un serveur Dovecot

Dovecot fournit une configuration sécurisée par défaut. Par exemple, TLS est activé par défaut pour transmettre des informations d'identification et des données cryptées sur les réseaux. Pour configurer TLS sur un serveur Dovecot, il suffit de définir les chemins d'accès aux fichiers de certificats et de clés privées. De plus, vous pouvez augmenter la sécurité des connexions TLS en générant et en utilisant les paramètres Diffie-Hellman pour fournir un secret parfait (PFS).

Conditions préalables

- Dovecot est installé.

- Les fichiers suivants ont été copiés aux emplacements indiqués sur le serveur :
  - Le certificat du serveur : **/etc/pki/dovecot/certs/server.example.com.crt**
  - La clé privée : **/etc/pki/dovecot/private/server.example.com.key**
  - Le certificat de l'autorité de certification (CA) : **/etc/pki/dovecot/certs/ca.crt**
- Le nom d'hôte figurant dans le champ **Subject DN** du certificat du serveur correspond au nom de domaine complet (FQDN) du serveur.

Procédure

1. Définir des autorisations sécurisées pour le fichier de la clé privée :

```
# chown root:root /etc/pki/dovecot/private/server.example.com.key
# chmod 600 /etc/pki/dovecot/private/server.example.com.key
```

2. Générer un fichier avec les paramètres Diffie-Hellman :

```
# openssl dhparam -out /etc/dovecot/dh.pem 4096
```

   En fonction du matériel et de l'entropie du serveur, la génération de paramètres Diffie-Hellman avec 4096 bits peut prendre plusieurs minutes.

3. Définissez les chemins d'accès aux fichiers de certificats et de clés privées dans le fichier **/etc/dovecot/conf.d/10-ssl.conf**:
   a. Mettez à jour les paramètres **ssl_cert** et **ssl_key** et définissez-les de manière à utiliser les chemins d'accès au certificat et à la clé privée du serveur :

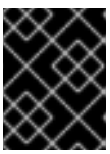
```
ssl_cert = </etc/pki/dovecot/certs/server.example.com.crt
ssl_key = </etc/pki/dovecot/private/server.example.com.key
```

   b. Décommentez le paramètre **ssl_ca** et définissez-le de manière à utiliser le chemin d'accès au certificat d'autorité de certification :

```
ssl_ca = </etc/pki/dovecot/certs/ca.crt
```

   c. Décommentez le paramètre **ssl_dh** et indiquez-lui le chemin d'accès au fichier des paramètres Diffie-Hellman :

```
ssl_dh = </etc/dovecot/dh.pem
```



IMPORTANT

Pour s'assurer que Dovecot lit la valeur d'un paramètre à partir d'un fichier, le chemin d'accès doit commencer par le caractère **<**.

Prochaine étape

- Préparer Dovecot à utiliser des utilisateurs virtuels

Ressources supplémentaires

- **/usr/share/doc/dovecot/wiki/SSL.DovecotConfiguration.txt**

1.2.3. Préparer Dovecot à utiliser des utilisateurs virtuels

Par défaut, Dovecot effectue de nombreuses actions sur le système de fichiers en tant qu'utilisateur du service. Cependant, configurer le back-end de Dovecot pour qu'il utilise un utilisateur local pour effectuer ces actions présente plusieurs avantages :

- Dovecot effectue des actions sur le système de fichiers en tant qu'utilisateur local spécifique au lieu d'utiliser l'ID de l'utilisateur (UID).
- Les utilisateurs n'ont pas besoin d'être disponibles localement sur le serveur.
- Vous pouvez stocker toutes les boîtes aux lettres et tous les fichiers spécifiques à l'utilisateur dans un répertoire racine.
- Les utilisateurs n'ont pas besoin d'un UID et d'un GID, ce qui réduit les efforts d'administration.
- Les utilisateurs qui ont accès au système de fichiers du serveur ne peuvent pas compromettre leurs boîtes aux lettres ou leurs index, car ils ne peuvent pas accéder à ces fichiers.
- La mise en place de la réplication est plus facile.

Conditions préalables

- Dovecot est installé.

Procédure

1. Créez l'utilisateur **vmail**:

   ```
   # useradd --home-dir /var/mail/ --shell /usr/sbin/nologin vmail
   ```

   Dovecot utilisera par la suite cet utilisateur pour gérer les boîtes aux lettres. Pour des raisons de sécurité, n'utilisez pas les utilisateurs du système **dovecot** ou **dovenull** à cette fin.

2. Si vous utilisez un chemin différent de celui de **/var/mail/**, définissez le contexte SELinux de **mail_spool_t**, par exemple :

   ```
   # semanage fcontext -a -t mail_spool_t "<path>(/.*)?"
   # restorecon -Rv <path>
   ```

3. Accordez les droits d'écriture sur **/var/mail/** uniquement à l'utilisateur **vmail**:

   ```
   # chown vmail:vmail /var/mail/
   # chmod 700 /var/mail/
   ```

4. Décommentez le paramètre **mail_location** dans le fichier **/etc/dovecot/conf.d/10-mail.conf** et attribuez-lui le format et l'emplacement de la boîte aux lettres :

   ```
   mail_location = sdbox:/var/mail/%n/
   ```

   Avec ce réglage :

- Dovecot utilise le format de boîte aux lettres **dbox** en mode **single**. Dans ce mode, le service stocke chaque courrier dans un fichier séparé, comme dans le format **maildir**.
- Dovecot résout la variable **%n** dans le chemin du nom d'utilisateur. Ceci est nécessaire pour s'assurer que chaque utilisateur dispose d'un répertoire séparé pour sa boîte aux lettres.

Prochaine étape

- Utilisation de LDAP comme backend d'authentification pour Dovecot .

Ressources supplémentaires

- **/usr/share/doc/dovecot/wiki/VirtualUsers.txt**
- **/usr/share/doc/dovecot/wiki/MailLocation.txt**
- **/usr/share/doc/dovecot/wiki/MailboxFormat.dbox.txt**
- **/usr/share/doc/dovecot/wiki/Variables.txt**

1.2.4. Utilisation de LDAP comme backend d'authentification pour Dovecot

Les utilisateurs d'un annuaire LDAP peuvent généralement s'authentifier auprès du service d'annuaire. Dovecot peut l'utiliser pour authentifier les utilisateurs lorsqu'ils se connectent aux services IMAP et POP3. Cette méthode d'authentification présente un certain nombre d'avantages :

- Les administrateurs peuvent gérer les utilisateurs de manière centralisée dans l'annuaire.
- Les comptes LDAP n'ont pas besoin d'attributs particuliers. Ils doivent seulement pouvoir s'authentifier auprès du serveur LDAP. Par conséquent, cette méthode est indépendante du système de stockage des mots de passe utilisé sur le serveur LDAP.
- Les utilisateurs n'ont pas besoin d'être disponibles localement sur le serveur via l'interface Name Service Switch (NSS) et le cadre PAM (Pluggable Authentication Modules).

Conditions préalables

- Dovecot est installé.
- La fonctionnalité des utilisateurs virtuels est configurée.
- Les connexions au serveur LDAP prennent en charge le cryptage TLS.
- RHEL sur le serveur Dovecot fait confiance au certificat de l'autorité de certification (CA) du serveur LDAP.
- Si les utilisateurs sont stockés dans différentes arborescences de l'annuaire LDAP, un compte LDAP dédié à Dovecot existe pour effectuer des recherches dans l'annuaire. Ce compte a besoin de permissions pour rechercher les Distinguished Names (DNs) des autres utilisateurs.

Procédure

1. Configurer les backends d'authentification dans le fichier **/etc/dovecot/conf.d/10-auth.conf**:
   a. Commentez les déclarations **include** pour les fichiers de configuration du backend d'authentification **auth-*.conf.ext** dont vous n'avez pas besoin, par exemple :

```
#!include auth-system.conf.ext
```

b. Activez l'authentification LDAP en décommentant la ligne suivante :

```
!include auth-ldap.conf.ext
```

2. Modifiez le fichier **/etc/dovecot/conf.d/auth-ldap.conf.ext** et ajoutez le paramètre **override_fields** comme suit à la section **userdb**:

```
userdb {
  driver = ldap
  args = /etc/dovecot/dovecot-ldap.conf.ext
  override_fields = uid=vmail gid=vmail home=/var/mail/%n/
}
```

En raison des valeurs fixes, Dovecot ne demande pas ces paramètres au serveur LDAP. Par conséquent, ces attributs n'ont pas non plus besoin d'être présents.

3. Créez le fichier **/etc/dovecot/dovecot-ldap.conf.ext** avec les paramètres suivants :

a. En fonction de la structure LDAP, configurez l'un des éléments suivants :

- Si les utilisateurs sont stockés dans différentes arborescences de l'annuaire LDAP, configurez des recherches dynamiques de DN :

```
dn = cn=dovecot_LDAP,dc=example,dc=com
dnpass = password
pass_filter = (&(objectClass=posixAccount)(uid=%n))
```

Dovecot utilise le DN, le mot de passe et le filtre spécifiés pour rechercher le DN de l'utilisateur s'authentifiant dans l'annuaire. Dans cette recherche, Dovecot remplace **%n** dans le filtre par le nom d'utilisateur. Notez que la recherche LDAP ne doit retourner qu'un seul résultat.

- Si tous les utilisateurs sont enregistrés sous une entrée spécifique, configurez un modèle DN :

```
auth_bind_userdn = cn=%n,ou=People,dc=example,dc=com
```

b. Activer l'authentification se lie au serveur LDAP pour vérifier les utilisateurs de Dovecot :

```
auth_bind = yes
```

c. Définir l'URL du serveur LDAP :

```
uris = ldaps://LDAP-srv.example.com
```

Pour des raisons de sécurité, n'utilisez que des connexions cryptées utilisant LDAPS ou la commande **STARTTLS** sur le protocole LDAP. Dans ce dernier cas, ajoutez **tls = yes** aux paramètres.

Pour que la validation du certificat fonctionne, le nom d'hôte du serveur LDAP doit correspondre au nom d'hôte utilisé dans son certificat TLS.

d. Activer la vérification du certificat TLS du serveur LDAP :

```
tls_require_cert = hard
```

e. Définissez le DN de base sur le DN où commencer la recherche d'utilisateurs :

```
base = ou=People,dc=example,dc=com
```

f. Définir l'étendue de la recherche :

```
scope = onelevel
```

Dovecot recherche avec la portée **onelevel** uniquement dans le DN de base spécifié et avec la portée **subtree** également dans les sous-arbres.

4. Définir des autorisations sécurisées sur le fichier **/etc/dovecot/dovecot-ldap.conf.ext**:

```
# chown root:root /etc/dovecot/dovecot-ldap.conf.ext
# chmod 600 /etc/dovecot/dovecot-ldap.conf.ext
```

Prochaine étape

- Terminez la configuration de Dovecot .

Ressources supplémentaires

- **/usr/share/doc/dovecot/example-config/dovecot-ldap.conf.ext**
- **/usr/share/doc/dovecot/wiki/UserDatabase.Static.txt**
- **/usr/share/doc/dovecot/wiki/AuthDatabase.LDAP.txt**
- **/usr/share/doc/dovecot/wiki/AuthDatabase.LDAP.AuthBinds.txt**
- **/usr/share/doc/dovecot/wiki/AuthDatabase.LDAP.PasswordLookups.txt**

1.2.5. Compléter la configuration de Dovecot

Une fois que vous avez installé et configuré Dovecot, ouvrez les ports requis dans le service **firewalld**, puis activez et démarrez le service. Vous pouvez ensuite tester le serveur.

Conditions préalables

- Les éléments suivants ont été configurés dans Dovecot :
  - Cryptage TLS
  - Un backend d'authentification
- Les clients font confiance au certificat de l'autorité de certification (AC).

Procédure

1. Si vous souhaitez fournir uniquement un service IMAP ou POP3 aux utilisateurs, décommentez le paramètre **protocols** dans le fichier **/etc/dovecot/dovecot.conf** et définissez-le en fonction des protocoles requis. Par exemple, si vous n'avez pas besoin de POP3, définissez :

```
protocols = imap lmtp
```

   Par défaut, les protocoles **imap**, **pop3** et **lmtp** sont activés.

2. Ouvrez les ports dans le pare-feu local. Par exemple, pour ouvrir les ports des protocoles IMAPS, IMAP, POP3S et POP3, entrez :

```
# firewall-cmd --permanent --add-service=imaps --add-service=imap --add-
service=pop3s --add-service=pop3
# firewall-cmd --reload
```

3. Activez et démarrez le service **dovecot**:

```
# systemctl enable --now dovecot
```

Vérification

1. Utilisez un client de messagerie, tel que Mozilla Thunderbird, pour vous connecter à Dovecot et lire les courriels. Les paramètres du client de messagerie dépendent du protocole que vous souhaitez utiliser :

   Tableau 1.2. Paramètres de connexion au serveur Dovecot

Protocol	Port	Sécurité des connexions	Méthode d'authentification
IMAP	143	STARTTLS	PLAIN[a]
IMAPS	993	SSL/TLS	PLAIN[a]
POP3	110	STARTTLS	PLAIN[a]
POP3S	995	SSL/TLS	PLAIN[a]

[a] Le client transmet des données cryptées via la connexion TLS. Par conséquent, les informations d'identification ne sont pas divulguées.

   Notez que ce tableau ne liste pas les paramètres pour les connexions non chiffrées car, par défaut, Dovecot n'accepte pas l'authentification en texte clair sur les connexions sans TLS.

2. Afficher les paramètres de configuration avec des valeurs autres que celles par défaut :

```
# doveconf -n
```

Ressources supplémentaires

- **firewall-cmd(1)** page de manuel

1.3. MISE EN PLACE D'UN SERVEUR DOVECOT AVEC AUTHENTIFICATION SQL MARIADB

Si vous stockez les utilisateurs et les mots de passe dans un serveur SQL MariaDB, vous pouvez configurer Dovecot pour qu'il l'utilise comme base de données des utilisateurs et comme backend d'authentification. Avec cette configuration, vous gérez les comptes de manière centralisée dans une base de données, et les utilisateurs n'ont pas d'accès local au système de fichiers sur le serveur Dovecot.

Les comptes gérés de manière centralisée sont également un avantage si vous envisagez de mettre en place plusieurs serveurs Dovecot avec réplication pour rendre vos boîtes aux lettres hautement disponibles.

1.3.1. Installation de Dovecot

Le paquet **dovecot** fournit :

- Le service **dovecot** et les services publics pour le maintenir
- Les services que Dovecot démarre à la demande, par exemple pour l'authentification
- Plugins, tels que le filtrage du courrier côté serveur
- Fichiers de configuration dans le répertoire **/etc/dovecot/**
- Documentation dans le répertoire **/usr/share/doc/dovecot/**

Procédure

- Installez le paquetage **dovecot**:

```
# dnf install dovecot
```

NOTE

Si Dovecot est déjà installé et que vous avez besoin de fichiers de configuration propres, renommez ou supprimez le répertoire **/etc/dovecot/**. Ensuite, réinstallez le paquetage. Sans supprimer les fichiers de configuration, la commande **dnf reinstall dovecot** ne réinitialise pas les fichiers de configuration dans **/etc/dovecot/**.

Prochaine étape

- Configuration du cryptage TLS sur un serveur Dovecot .

1.3.2. Configuration du cryptage TLS sur un serveur Dovecot

Dovecot fournit une configuration sécurisée par défaut. Par exemple, TLS est activé par défaut pour transmettre des informations d'identification et des données cryptées sur les réseaux. Pour configurer TLS sur un serveur Dovecot, il suffit de définir les chemins d'accès aux fichiers de certificats et de clés privées. De plus, vous pouvez augmenter la sécurité des connexions TLS en générant et en utilisant les paramètres Diffie-Hellman pour fournir un secret parfait (PFS).

Conditions préalables

- Dovecot est installé.
- Les fichiers suivants ont été copiés aux emplacements indiqués sur le serveur :
  - Le certificat du serveur : **/etc/pki/dovecot/certs/server.example.com.crt**
  - La clé privée : **/etc/pki/dovecot/private/server.example.com.key**
  - Le certificat de l'autorité de certification (CA) : **/etc/pki/dovecot/certs/ca.crt**
- Le nom d'hôte figurant dans le champ **Subject DN** du certificat du serveur correspond au nom de domaine complet (FQDN) du serveur.

Procédure

1. Définir des autorisations sécurisées pour le fichier de la clé privée :

```
# chown root:root /etc/pki/dovecot/private/server.example.com.key
# chmod 600 /etc/pki/dovecot/private/server.example.com.key
```

2. Générer un fichier avec les paramètres Diffie-Hellman :

```
# openssl dhparam -out /etc/dovecot/dh.pem 4096
```

   En fonction du matériel et de l'entropie du serveur, la génération de paramètres Diffie-Hellman avec 4096 bits peut prendre plusieurs minutes.

3. Définissez les chemins d'accès aux fichiers de certificats et de clés privées dans le fichier **/etc/dovecot/conf.d/10-ssl.conf**:
   a. Mettez à jour les paramètres **ssl_cert** et **ssl_key** et définissez-les de manière à utiliser les chemins d'accès au certificat et à la clé privée du serveur :

```
ssl_cert = </etc/pki/dovecot/certs/server.example.com.crt
ssl_key = </etc/pki/dovecot/private/server.example.com.key
```

   b. Décommentez le paramètre **ssl_ca** et définissez-le de manière à utiliser le chemin d'accès au certificat d'autorité de certification :

```
ssl_ca = </etc/pki/dovecot/certs/ca.crt
```

   c. Décommentez le paramètre **ssl_dh** et indiquez-lui le chemin d'accès au fichier des paramètres Diffie-Hellman :

```
ssl_dh = </etc/dovecot/dh.pem
```

IMPORTANT

Pour s'assurer que Dovecot lit la valeur d'un paramètre à partir d'un fichier, le chemin d'accès doit commencer par le caractère **<**.

Prochaine étape

- Préparer Dovecot à utiliser des utilisateurs virtuels

Ressources supplémentaires

- **/usr/share/doc/dovecot/wiki/SSL.DovecotConfiguration.txt**

1.3.3. Préparer Dovecot à utiliser des utilisateurs virtuels

Par défaut, Dovecot effectue de nombreuses actions sur le système de fichiers en tant qu'utilisateur du service. Cependant, configurer le back-end de Dovecot pour qu'il utilise un utilisateur local pour effectuer ces actions présente plusieurs avantages :

- Dovecot effectue des actions sur le système de fichiers en tant qu'utilisateur local spécifique au lieu d'utiliser l'ID de l'utilisateur (UID).
- Les utilisateurs n'ont pas besoin d'être disponibles localement sur le serveur.
- Vous pouvez stocker toutes les boîtes aux lettres et tous les fichiers spécifiques à l'utilisateur dans un répertoire racine.
- Les utilisateurs n'ont pas besoin d'un UID et d'un GID, ce qui réduit les efforts d'administration.
- Les utilisateurs qui ont accès au système de fichiers du serveur ne peuvent pas compromettre leurs boîtes aux lettres ou leurs index, car ils ne peuvent pas accéder à ces fichiers.
- La mise en place de la réplication est plus facile.

Conditions préalables

- Dovecot est installé.

Procédure

1. Créez l'utilisateur **vmail**:

```
# useradd --home-dir /var/mail/ --shell /usr/sbin/nologin vmail
```

   Dovecot utilisera par la suite cet utilisateur pour gérer les boîtes aux lettres. Pour des raisons de sécurité, n'utilisez pas les utilisateurs du système **dovecot** ou **dovenull** à cette fin.

2. Si vous utilisez un chemin différent de celui de **/var/mail/**, définissez le contexte SELinux de **mail_spool_t**, par exemple :

```
# semanage fcontext -a -t mail_spool_t "<path>(/.*)?"
# restorecon -Rv <path>
```

3. Accordez les droits d'écriture sur **/var/mail/** uniquement à l'utilisateur **vmail**:

```
# chown vmail:vmail /var/mail/
# chmod 700 /var/mail/
```

4. Décommentez le paramètre **mail_location** dans le fichier **/etc/dovecot/conf.d/10-mail.conf** et attribuez-lui le format et l'emplacement de la boîte aux lettres :

```
mail_location = sdbox:/var/mail/%n/
```

   Avec ce réglage :

- Dovecot utilise le format de boîte aux lettres **dbox** en mode **single**. Dans ce mode, le service stocke chaque courrier dans un fichier séparé, comme dans le format **maildir**.
- Dovecot résout la variable **%n** dans le chemin du nom d'utilisateur. Ceci est nécessaire pour s'assurer que chaque utilisateur dispose d'un répertoire séparé pour sa boîte aux lettres.

Prochaine étape

- Utilisation d'une base de données SQL MariaDB comme backend d'authentification Dovecot

Ressources supplémentaires

- **/usr/share/doc/dovecot/wiki/VirtualUsers.txt**
- **/usr/share/doc/dovecot/wiki/MailLocation.txt**
- **/usr/share/doc/dovecot/wiki/MailboxFormat.dbox.txt**
- **/usr/share/doc/dovecot/wiki/Variables.txt**

1.3.4. Utilisation d'une base de données SQL MariaDB comme backend d'authentification Dovecot

Dovecot peut lire les comptes et les mots de passe d'une base de données MariaDB et les utiliser pour authentifier les utilisateurs lorsqu'ils se connectent au service IMAP ou POP3. Les avantages de cette méthode d'authentification sont les suivants

- Les administrateurs peuvent gérer les utilisateurs de manière centralisée dans une base de données.
- Les utilisateurs n'ont pas d'accès local au serveur.

Conditions préalables

- Dovecot est installé.
- La fonctionnalité des utilisateurs virtuels est configurée.
- Les connexions au serveur MariaDB prennent en charge le cryptage TLS.
- La base de données **dovecotDB** existe dans MariaDB, et la table **users** contient au moins une colonne **username** et **password**.
- La colonne **password** contient des mots de passe cryptés avec un schéma supporté par Dovecot.
- Les mots de passe utilisent le même schéma ou ont un **{*pw-storage-scheme*}** préfixe.
- L'utilisateur MariaDB **dovecot** a le droit de lire la table **users** dans la base de données **dovecotDB**.
- Le certificat de l'autorité de certification (CA) qui a émis le certificat TLS du serveur MariaDB est stocké sur le serveur Dovecot dans le fichier **/etc/pki/tls/certs/ca.crt**.

Procédure

1. Installez le paquetage **dovecot-mysql**:

```
# dnf install dovecot-mysql
```

2. Configurer les backends d'authentification dans le fichier **/etc/dovecot/conf.d/10-auth.conf**:

   a. Commentez les déclarations **include** pour les fichiers de configuration du backend d'authentification **auth-*.conf.ext** dont vous n'avez pas besoin, par exemple :

   ```
   #!include auth-system.conf.ext
   ```

   b. Activez l'authentification SQL en décommentant la ligne suivante :

   ```
   !include auth-sql.conf.ext
   ```

3. Modifiez le fichier **/etc/dovecot/conf.d/auth-sql.conf.ext** et ajoutez le paramètre **override_fields** à la section **userdb** comme suit :

```
userdb {
  driver = sql
  args = /etc/dovecot/dovecot-sql.conf.ext
  override_fields = uid=vmail gid=vmail home=/var/mail/%n/
}
```

   En raison des valeurs fixes, Dovecot n'interroge pas ces paramètres à partir du serveur SQL.

4. Créez le fichier **/etc/dovecot/dovecot-sql.conf.ext** avec les paramètres suivants :

```
driver = mysql
connect = host=mariadb_srv.example.com dbname=dovecotDB user=dovecot
password=dovecotPW ssl_ca=/etc/pki/tls/certs/ca.crt
default_pass_scheme = SHA512-CRYPT
user_query = SELECT username FROM users WHERE username='%u';
password_query = SELECT username AS user, password FROM users WHERE
username='%u';
iterate_query = SELECT username FROM users;
```

   Pour utiliser le cryptage TLS vers le serveur de base de données, définissez l'option **ssl_ca** sur le chemin du certificat de l'autorité de certification qui a émis le certificat du serveur MariaDB. Pour que la validation du certificat fonctionne, le nom d'hôte du serveur MariaDB doit correspondre au nom d'hôte utilisé dans son certificat TLS.

   Si les valeurs du mot de passe dans la base de données contiennent un préfixe **{*pw-storage-scheme*}** vous pouvez omettre le paramètre **default_pass_scheme**.

   Les requêtes dans le fichier doivent être définies comme suit :

   - Pour le paramètre **user_query**, la requête doit retourner le nom d'utilisateur de l'utilisateur Dovecot. La requête ne doit également renvoyer qu'un seul résultat.

   - Pour le paramètre **password_query**, la requête doit retourner le nom d'utilisateur et le mot de passe, et Dovecot doit utiliser ces valeurs dans les variables **user** et **password**. Par conséquent, si la base de données utilise des noms de colonnes différents, utilisez la commande SQL **AS** pour renommer une colonne dans le résultat.

- Pour le paramètre **iterate_query**, la requête doit renvoyer une liste de tous les utilisateurs.

5. Définir des autorisations sécurisées sur le fichier **/etc/dovecot/dovecot-sql.conf.ext**:

```
# chown root:root /etc/dovecot/dovecot-sql.conf.ext
# chmod 600 /etc/dovecot/dovecot-sql.conf.ext
```

Prochaine étape

- Terminez la configuration de Dovecot .

Ressources supplémentaires

- **/usr/share/doc/dovecot/example-config/dovecot-sql.conf.ext**
- **/usr/share/doc/dovecot/wiki/Authentication.PasswordSchemes.txt**

1.3.5. Compléter la configuration de Dovecot

Une fois que vous avez installé et configuré Dovecot, ouvrez les ports requis dans le service **firewalld**, puis activez et démarrez le service. Vous pouvez ensuite tester le serveur.

Conditions préalables

- Les éléments suivants ont été configurés dans Dovecot :
  - Cryptage TLS
  - Un backend d'authentification
- Les clients font confiance au certificat de l'autorité de certification (AC).

Procédure

1. Si vous souhaitez fournir uniquement un service IMAP ou POP3 aux utilisateurs, décommentez le paramètre **protocols** dans le fichier **/etc/dovecot/dovecot.conf** et définissez-le en fonction des protocoles requis. Par exemple, si vous n'avez pas besoin de POP3, définissez :

```
protocols = imap lmtp
```

   Par défaut, les protocoles **imap**, **pop3** et **lmtp** sont activés.

2. Ouvrez les ports dans le pare-feu local. Par exemple, pour ouvrir les ports des protocoles IMAPS, IMAP, POP3S et POP3, entrez :

```
# firewall-cmd --permanent --add-service=imaps --add-service=imap --add-
service=pop3s --add-service=pop3
# firewall-cmd --reload
```

3. Activez et démarrez le service **dovecot**:

```
# systemctl enable --now dovecot
```

Vérification

1. Utilisez un client de messagerie, tel que Mozilla Thunderbird, pour vous connecter à Dovecot et lire les courriels. Les paramètres du client de messagerie dépendent du protocole que vous souhaitez utiliser :

   Tableau 1.3. Paramètres de connexion au serveur Dovecot

Protocol	Port	Sécurité des connexions	Méthode d'authentification
IMAP	143	STARTTLS	PLAIN[a]
IMAPS	993	SSL/TLS	PLAIN[a]
POP3	110	STARTTLS	PLAIN[a]
POP3S	995	SSL/TLS	PLAIN[a]

[a] Le client transmet des données cryptées via la connexion TLS. Par conséquent, les informations d'identification ne sont pas divulguées.

   Notez que ce tableau ne liste pas les paramètres pour les connexions non chiffrées car, par défaut, Dovecot n'accepte pas l'authentification en texte clair sur les connexions sans TLS.

2. Afficher les paramètres de configuration avec des valeurs autres que celles par défaut :

```
# doveconf -n
```

Ressources supplémentaires

- **firewall-cmd(1)** page de manuel

1.4. CONFIGURATION DE LA RÉPLICATION ENTRE DEUX SERVEURS DOVECOT

Avec la réplication bidirectionnelle, vous pouvez rendre votre serveur Dovecot hautement disponible, et les clients IMAP et POP3 peuvent accéder à une boîte aux lettres sur les deux serveurs. Dovecot suit les changements dans les journaux d'indexation de chaque boîte aux lettres et résout les conflits de manière sûre.

Effectuez cette procédure sur les deux partenaires de réplication.

NOTE

La réplication ne fonctionne qu'entre paires de serveurs. Par conséquent, dans un grand cluster, vous avez besoin de plusieurs paires de serveurs indépendants.

Conditions préalables

- Les deux serveurs utilisent le même backend d'authentification. Il est préférable d'utiliser LDAP ou SQL pour gérer les comptes de manière centralisée.
- La configuration de la base de données des utilisateurs de Dovecot supporte le listing des utilisateurs. Utilisez la commande **doveadm user '*'** pour le vérifier.
- Dovecot accède aux boîtes aux lettres sur le système de fichiers en tant qu'utilisateur **vmail** au lieu de l'ID de l'utilisateur (UID).

Procédure

1. Créez le fichier **/etc/dovecot/conf.d/10-replication.conf** et effectuez-y les étapes suivantes :
   a. Activez les plug-ins **notify** et **replication**:

```
mail_plugins = $mail_plugins notify replication
```

   b. Ajouter une section **service replicator**:

```
service replicator {
  process_min_avail = 1

  unix_listener replicator-doveadm {
    mode = 0600
    user = vmail
  }
}
```

   Avec ces paramètres, Dovecot démarre au moins un processus réplicateur lorsque le service **dovecot** démarre. De plus, cette section définit les paramètres du socket **replicator-doveadm**.

   c. Ajoutez une section **service aggregator** pour configurer le tuyau **replication-notify-fifo** et la prise **replication-notify**:

```
service aggregator {
  fifo_listener replication-notify-fifo {
    user = vmail
  }
  unix_listener replication-notify {
    user = vmail
  }
}
```

   d. Ajouter une section **service doveadm** pour définir le port du service de réplication :

```
service doveadm {
  inet_listener {
    port = 12345
  }
}
```

   e. Définir le mot de passe du service de réplication **doveadm**:

```
doveadm_password = replication_password
```

–

Le mot de passe doit être le même sur les deux serveurs.

f. Configurer le partenaire de réplication :

```
plugin {
  mail_replica = tcp:server2.example.com:12345
}
```

g. Facultatif : Définir le nombre maximum de processus parallèles **dsync**:

```
replication_max_conns = 20
```

La valeur par défaut de **replication_max_conns** est **10**.

2. Définir des autorisations sécurisées sur le fichier **/etc/dovecot/conf.d/10-replication.conf**:

```
# chown root:root /etc/dovecot/conf.d/10-replication.conf
# chmod 600 /etc/dovecot/conf.d/10-replication.conf
```

3. Activez le booléen SELinux **nis_enabled** pour permettre à Dovecot d'ouvrir le port de réplication **doveadm**:

```
setsebool -P nis_enabled on
```

4. Configurez les règles **firewalld** pour autoriser uniquement le partenaire de réplication à accéder au port de réplication, par exemple :

```
# firewall-cmd --permanent --zone=public --add-rich-rule="rule family="ipv4" source
address="192.0.2.1/32" port protocol="tcp" port="12345" accept"
# firewall-cmd --permanent --zone=public --add-rich-rule="rule family="ipv6" source
address="2001:db8:2::1/128" port protocol="tcp" port="12345" accept"
# firewall-cmd --reload
```

Les masques de sous-réseau **/32** pour l'adresse IPv4 et **/128** pour l'adresse IPv6 limitent l'accès aux adresses spécifiées.

5. Effectuez également cette procédure sur l'autre partenaire de réplication.

6. Recharger Dovecot :

```
# systemctl reload dovecot
```

Vérification

1. Effectuer une action dans une boîte aux lettres sur un serveur et vérifier ensuite si Dovecot a répliqué la modification sur l'autre serveur.

2. Affiche l'état du réplicateur :

```
# doveadm replicator status
Queued 'sync' requests       0
Queued 'high' requests       0
Queued 'low' requests        0
```

```
Queued 'failed' requests      0
Queued 'full resync' requests 30
Waiting 'failed' requests     0
Total number of known users   75
```

3. Affiche l'état des réplicateurs d'un utilisateur spécifique :

```
# doveadm replicator status example_user
username        priority  fast sync  full sync  success sync  failed
example_user    none      02:05:28   04:19:07   02:05:28      -
```

Ressources supplémentaires

- **dsync(1)** page de manuel
- **/usr/share/doc/dovecot/wiki/Replication.txt**

1.5. ABONNEMENT AUTOMATIQUE DES UTILISATEURS AUX BOÎTES AUX LETTRES IMAP

Typiquement, les administrateurs de serveurs IMAP veulent que Dovecot crée automatiquement certaines boîtes aux lettres, telles que **Sent** et **Trash**, et y abonne les utilisateurs. Vous pouvez définir cela dans les fichiers de configuration.

En outre, vous pouvez définir *special-use mailboxes*. Les clients IMAP permettent souvent de définir des boîtes aux lettres à des fins particulières, par exemple pour les courriers électroniques envoyés. Pour éviter que l'utilisateur ne doive sélectionner et définir manuellement les boîtes aux lettres correctes, les serveurs IMAP peuvent envoyer un attribut **special-use** dans la commande IMAP **LIST**. Les clients peuvent alors utiliser cet attribut pour identifier et définir, par exemple, la boîte aux lettres pour les courriers électroniques envoyés.

Conditions préalables

- Dovecot est configuré.

Procédure

1. Mettre à jour la section de l'espace de noms **inbox** dans le fichier **/etc/dovecot/conf.d/15-mailboxes.conf**:

   a. Ajoutez le paramètre **auto = subscribe** à chaque boîte aux lettres à usage spécial qui doit être accessible aux utilisateurs, par exemple :

```
namespace inbox {
  ...
  mailbox Drafts {
    special_use = \Drafts
    auto = subscribe
  }

  mailbox Junk {
    special_use = \Junk
    auto = subscribe
  }
```

```
  mailbox Trash {
    special_use = \Trash
    auto = subscribe
  }

  mailbox Sent {
    special_use = \Sent
    auto = subscribe
  }
  ...
}
```

Si vos clients de messagerie supportent d'autres boîtes aux lettres à usage spécial, vous pouvez ajouter des entrées similaires. Le paramètre **special_use** définit la valeur que Dovecot envoie dans l'attribut **special-use** aux clients.

b. Facultatif : si vous souhaitez définir d'autres boîtes aux lettres qui n'ont pas d'utilité particulière, ajoutez-leur des sections **mailbox** dans la boîte de réception de l'utilisateur, par exemple :

```
namespace inbox {
  ...
  mailbox "Important Emails" {
    auto = <value>
  }
  ...
}
```

Le paramètre **auto** peut être réglé sur l'une des valeurs suivantes :

- **subscribe**: Crée automatiquement la boîte aux lettres et y inscrit l'utilisateur.
- **create**: Crée automatiquement la boîte aux lettres sans y inscrire l'utilisateur.
- **no** (par défaut) : Dovecot ne crée pas la boîte aux lettres et n'y inscrit pas l'utilisateur.

2. Recharger Dovecot :

```
# systemctl reload dovecot
```

Vérification

- Utilisez un client IMAP et accédez à votre boîte aux lettres.
  Les boîtes aux lettres dont le paramètre est **auto = subscribe** sont automatiquement visibles. Si le client prend en charge les boîtes aux lettres à usage spécial et les objectifs définis, il les utilise automatiquement.

Ressources supplémentaires

- RFC 6154 : Extension IMAP LIST pour les boîtes aux lettres à usage spécial
- **/usr/share/doc/dovecot/wiki/MailboxSettings.txt**

1.6. CONFIGURATION D'UNE SOCKET LMTP ET D'UN LISTENER LMTPS

Les serveurs SMTP, tels que Postfix, utilisent le protocole LMTP (Local Mail Transfer Protocol) pour délivrer les emails à Dovecot. Si le serveur SMTP fonctionne :

- Sur le même hôte que Dovecot, utilisez un socket LMTP
- Sur un autre hôte, utilisez un service LMTP
  Par défaut, le protocole LMTP n'est pas chiffré. Cependant, si vous avez configuré le cryptage TLS, Dovecot utilise automatiquement les mêmes paramètres pour le service LMTP. Les serveurs SMTP peuvent alors s'y connecter en utilisant le protocole LMTPS ou la commande **STARTTLS** sur LMTP.

Conditions préalables

- Dovecot est installé.
- Si vous souhaitez configurer un service LMTP, le chiffrement TLS est configuré dans Dovecot.

Procédure

1. Vérifiez que le protocole LMTP est activé :

   ```
   # doveconf -a | egrep "^protocols"
   protocols = imap pop3 lmtp
   ```

   Le protocole est activé si la sortie contient **lmtp**.

2. Si le protocole **lmtp** est désactivé, modifiez le fichier **/etc/dovecot/dovecot.conf** et ajoutez **lmtp** aux valeurs du paramètre **protocols**:

   ```
   protocoles = ... lmtp
   ```

3. Selon que vous avez besoin d'un socket ou d'un service LMTP, apportez les modifications suivantes à la section **service lmtp** du fichier **/etc/dovecot/conf.d/10-master.conf**:

   - Socket LMTP : Par défaut, Dovecot crée automatiquement le socket **/var/run/dovecot/lmtp**.
     Facultatif : Personnalisez la propriété et les autorisations :

     ```
     service lmtp {
       ...
       unix_listener lmtp {
         mode = 0600
         user = postfix
         group = postfix
       }
       ...
     }
     ```

   - Service LMTP : Ajouter une sous-section **inet_listener**:

     ```
     service lmtp {
     ```

```
  ...
  inet_listener lmtp {
    port = 24
  }
  ...
}
```

4. Configurez les règles **firewalld** pour autoriser uniquement le serveur SMTP à accéder au port LMTP, par exemple :

```
# firewall-cmd --permanent --zone=public --add-rich-rule="rule family="ipv4" source
address="192.0.2.1/32" port protocol="tcp" port="24" accept"
# firewall-cmd --permanent --zone=public --add-rich-rule="rule family="ipv6" source
address="2001:db8:2::1/128" port protocol="tcp" port="24" accept"
# firewall-cmd --reload
```

   Les masques de sous-réseau **/32** pour l'adresse IPv4 et **/128** pour l'adresse IPv6 limitent l'accès aux adresses spécifiées.

5. Recharger Dovecot :

```
# systemctl reload dovecot
```

Vérification

1. Si vous avez configuré le socket LMTP, vérifiez que Dovecot a créé le socket et que les permissions sont correctes :

```
# ls -l /var/run/dovecot/lmtp
srw-------. 1 postfix postfix 0 Nov 22 17:17 /var/run/dovecot/lmtp
```

2. Configurez le serveur SMTP pour qu'il soumette les emails à Dovecot en utilisant le socket ou le service LMTP.
   Lorsque vous utilisez le service LMTP, assurez-vous que le serveur SMTP utilise le protocole LMTPS ou envoie la commande **STARTTLS** pour utiliser une connexion cryptée.

Ressources supplémentaires

- **/usr/share/doc/dovecot/wiki/LMTP.txt**

1.7. DÉSACTIVER LE SERVICE IMAP OU POP3 DANS DOVECOT

Par défaut, Dovecot fournit les services IMAP et POP3. Si vous n'avez besoin que de l'un d'entre eux, vous pouvez désactiver l'autre pour réduire la surface d'attaque.

Conditions préalables

- Dovecot est installé.

Procédure

1. Décommentez le paramètre **protocols** dans le fichier **/etc/dovecot/dovecot.conf** et définissez-le de manière à utiliser les protocoles requis. Par exemple, si vous n'avez pas besoin de POP3, définissez :

```
protocols = imap lmtp
```

   Par défaut, les protocoles **imap**, **pop3** et **lmtp** sont activés.

2. Recharger Dovecot :

```
# systemctl reload dovecot
```

3. Fermez les ports qui ne sont plus nécessaires dans le pare-feu local. Par exemple, pour fermer les ports des protocoles POP3S et POP3, entrez :

```
# firewall-cmd --remove-service=pop3s --remove-service=pop3
# firewall-cmd --reload
```

Vérification

- Affiche tous les ports en mode **LISTEN** ouverts par le processus **dovecot**:

```
# ss -tulp | grep dovecot
tcp  LISTEN 0  100  0.0.0.0:993  0.0.0.0:*  users:(("dovecot",pid=1405,fd=44))
tcp  LISTEN 0  100  0.0.0.0:143  0.0.0.0:*  users:(("dovecot",pid=1405,fd=42))
tcp  LISTEN 0  100     [::]:993     [::]:*  users:(("dovecot",pid=1405,fd=45))
tcp  LISTEN 0  100     [::]:143     [::]:*  users:(("dovecot",pid=1405,fd=43))
```

  Dans cet exemple, Dovecot n'écoute que sur les ports TCP **993** (IMAPS) et **143** (IMAP).

  Notez que Dovecot n'ouvre un port pour le protocole LMTP que si vous configurez le service pour qu'il écoute sur un port au lieu d'utiliser un socket.

Ressources supplémentaires

- **firewall-cmd(1)** page de manuel

1.8. ACTIVATION DU FILTRAGE DES EMAILS CÔTÉ SERVEUR À L'AIDE DE SIEVE SUR UN SERVEUR IMAP DOVECOT

Vous pouvez télécharger des scripts Sieve sur un serveur à l'aide du protocole ManageSieve. Les scripts Sieve définissent les règles et les actions qu'un serveur doit valider et exécuter sur les courriers électroniques entrants. Par exemple, les utilisateurs peuvent utiliser Sieve pour transférer les courriels provenant d'un expéditeur spécifique, et les administrateurs peuvent créer un filtre global pour déplacer les courriels signalés par un filtre anti-spam dans un dossier IMAP distinct.

Le plugin **ManageSieve** ajoute le support des scripts Sieve et du protocole ManageSieve à un serveur IMAP Dovecot.

AVERTISSEMENT

N'utilisez que des clients qui prennent en charge l'utilisation du protocole ManageSieve sur des connexions TLS. La désactivation de TLS pour ce protocole entraîne l'envoi par les clients d'informations d'identification en texte clair sur le réseau.

Conditions préalables

- Dovecot est configuré et fournit des boîtes aux lettres IMAP.
- Le chiffrement TLS est configuré dans Dovecot.
- Les clients de messagerie prennent en charge le protocole ManageSieve sur les connexions TLS.

Procédure

1. Installez le paquetage **dovecot-pigeonhole**:

```
# dnf install dovecot-pigeonhole
```

2. Décommentez la ligne suivante dans **/etc/dovecot/conf.d/20-managesieve.conf** pour activer le protocole **sieve**:

```
protocols = $protocols sieve
```

   Ce paramètre active Sieve en plus des autres protocoles déjà activés.

3. Ouvrez le port ManageSieve dans **firewalld**:

```
# firewall-cmd --permanent --add-service=managesieve
# firewall-cmd --reload
```

4. Recharger Dovecot :

```
# systemctl reload dovecot
```

Vérification

1. Utilisez un client et téléchargez un script Sieve. Utilisez les paramètres de connexion suivants :
   - Port : 4190
   - Sécurité de la connexion : SSL/TLS
   - Méthode d'authentification : PLAIN
2. Envoyez un courriel à l'utilisateur qui a téléchargé le script Sieve. Si le courriel correspond aux règles du script, vérifiez que le serveur exécute les actions définies.

Ressources supplémentaires

- **/usr/share/doc/dovecot/wiki/Pigeonhole.Sieve.Plugins.IMAPSieve.txt**
- **/usr/share/doc/dovecot/wiki/Pigeonhole.Sieve.Troubleshooting.txt**
- **firewall-cmd(1)** page de manuel

1.9. COMMENT DOVECOT TRAITE LES FICHIERS DE CONFIGURATION

Le paquetage **dovecot** fournit le fichier de configuration principal **/etc/dovecot/dovecot.conf** et plusieurs fichiers de configuration dans le répertoire **/etc/dovecot/conf.d/**. Dovecot combine les fichiers pour construire la configuration lorsque vous démarrez le service.

Le principal avantage de plusieurs fichiers de configuration est de regrouper les paramètres et d'améliorer la lisibilité. Si vous préférez un seul fichier de configuration, vous pouvez conserver tous les paramètres dans **/etc/dovecot/dovecot.conf** et supprimer toutes les déclarations de **include** et **include_try** dans ce fichier.

Ressources supplémentaires

- **/usr/share/doc/dovecot/wiki/ConfigFile.txt**
- **/usr/share/doc/dovecot/wiki/Variables.txt**