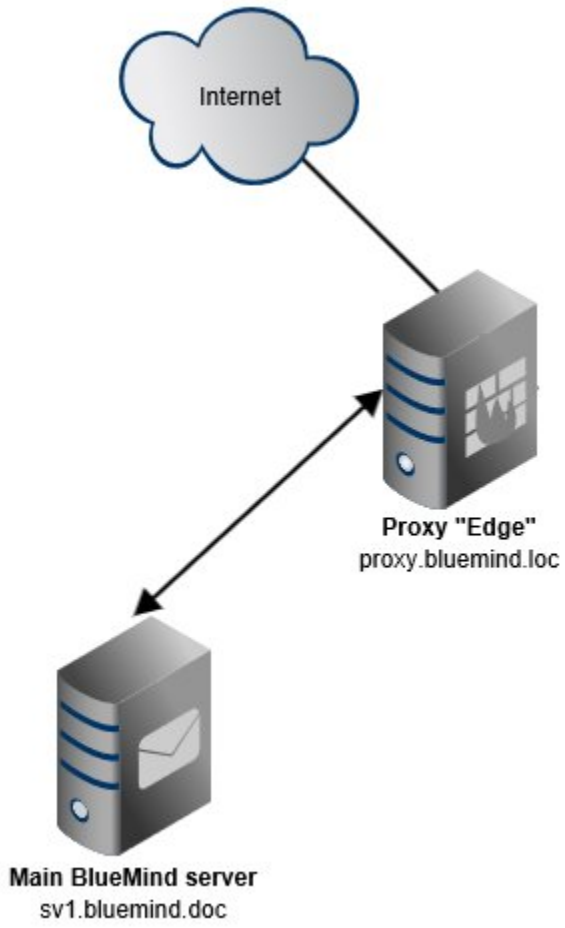
INSTALLATION D'UN SERVEUR EDGE : NGINX ET POSTFIX

PRÉSENTATION

Le présent document a pour but de décrire la procédure de déploiement d'un serveur de type Edge BlueMind comme relai postfix et proxy.

PRINCIPE

- BlueMind est installé sur le serveur principal
- le rôle *bm-edge-role* est installé sur le serveur dit "*Edge*"
- le serveur web nginx du serveur edge est configuré comme relai proxy servant le serveur principal



PROCÉDURE DE DÉPLOIEMENT

1. Installer BlueMind sur le serveur principal en suivant la procédure habituelle

   ⚠ L'espace de stockage des backups de BlueMind doit être accessible sur ce nouveau serveur sous */var/backups/bluemind*

2. installer la souscription sur le serveur secondaire en tant que fichier

> Rappel : le fichier texte correspondant à la souscription peut être installé manuellement sur un serveur
>
> - pour Ubuntu / Debian en tant que `/etc/apt/sources.list.d/bm.list`
> - pour RedHat / CentOS en tant que `/etc/yum.repos.d/bm.repo`

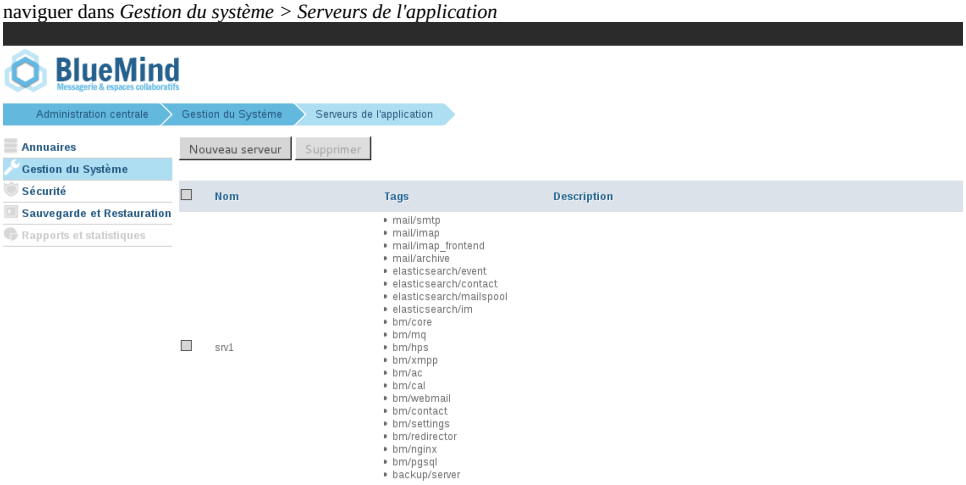
3. installer le paquet `bm-edge-role` sur le serveur edge :

Debian/Ubuntu RedHat/CentOS

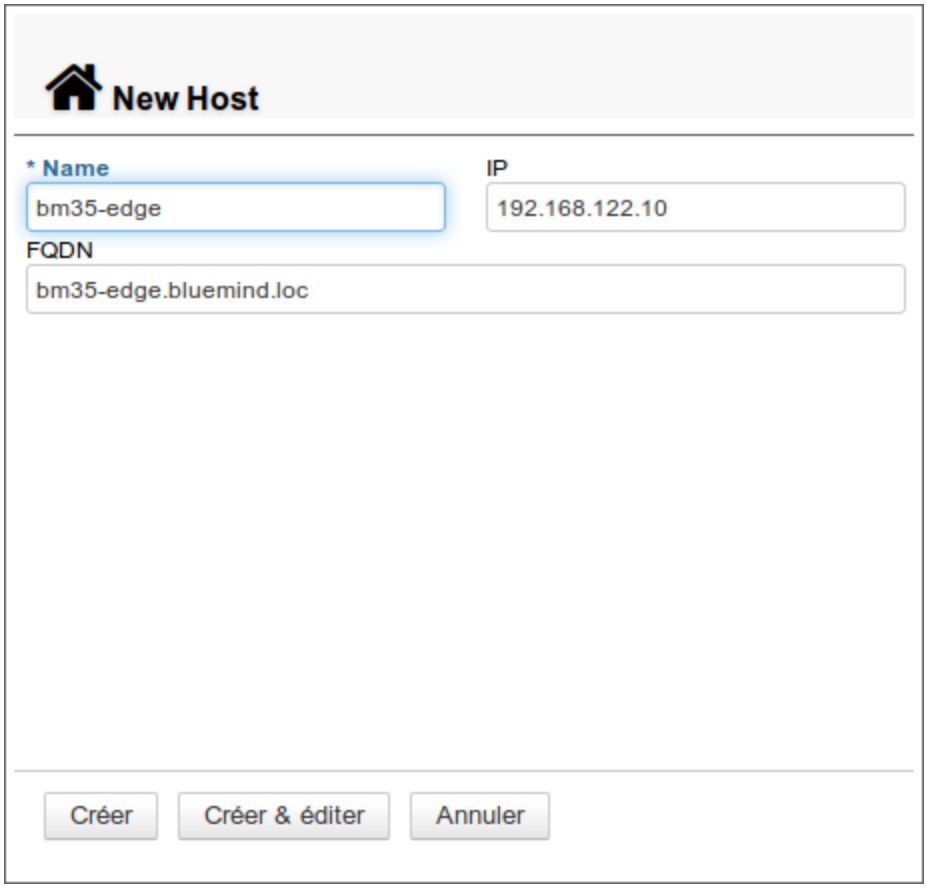
```
bm35-edge.bluemind.loc:~$ sudo aptitude update
bm35-edge.bluemind.loc:~$ sudo aptitude install bm-edge-role
```

```
bm35-edge.bluemind.loc:~$ sudo yum makecache
bm35-edge.bluemind.loc:~$ sudo yum install bm-edge-role
```

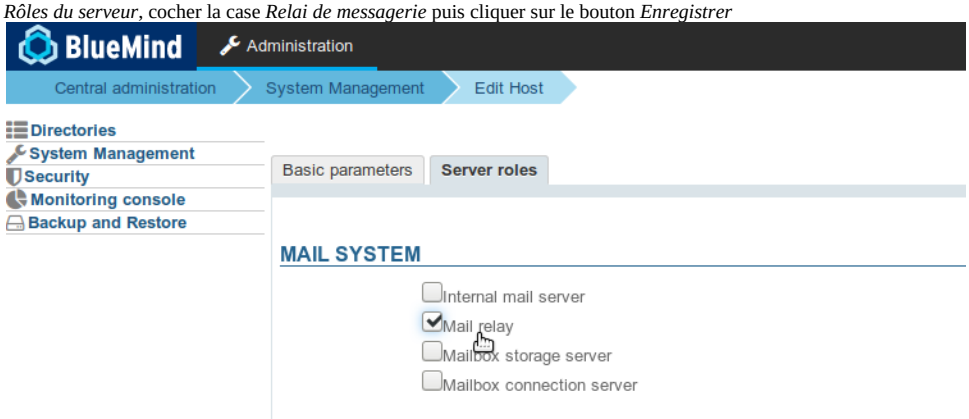
4. ajouter le rôle de relai smtp au serveur edge dans le panneau d'administration du serveur principal :
   - se connecter à BlueMind sur le serveur principal avec l'utilisateur *admin0@global.virt*
   - naviguer dans *Gestion du système > Serveurs de l'application*



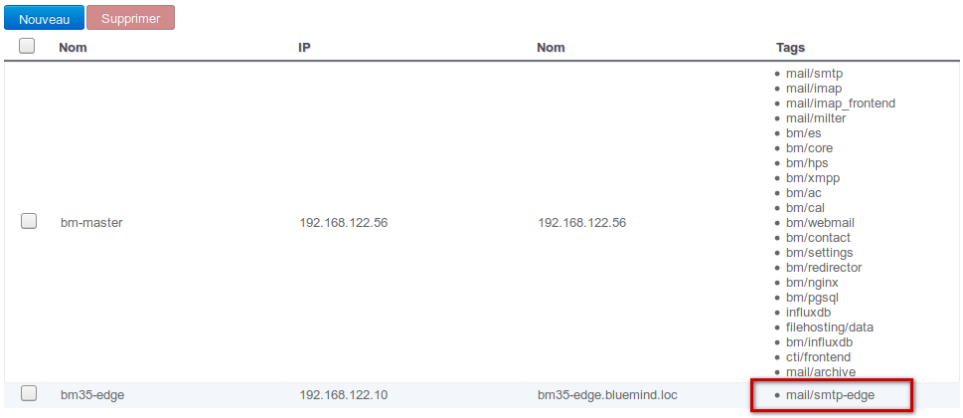
   - cliquer sur le bouton *Nouveau > Serveur*
   - remplir les informations du nouveau serveur et cliquer sur *Créer*



- cliquer sur "Créer & éditer" ou sur "Créer" puis, une fois de retour à la liste des serveurs, cliquer sur la ligne correspondant à celui-ci dans l'onglet *Rôles du serveur*, cocher la case *Relai de messagerie* puis cliquer sur le bouton *Enregistrer*

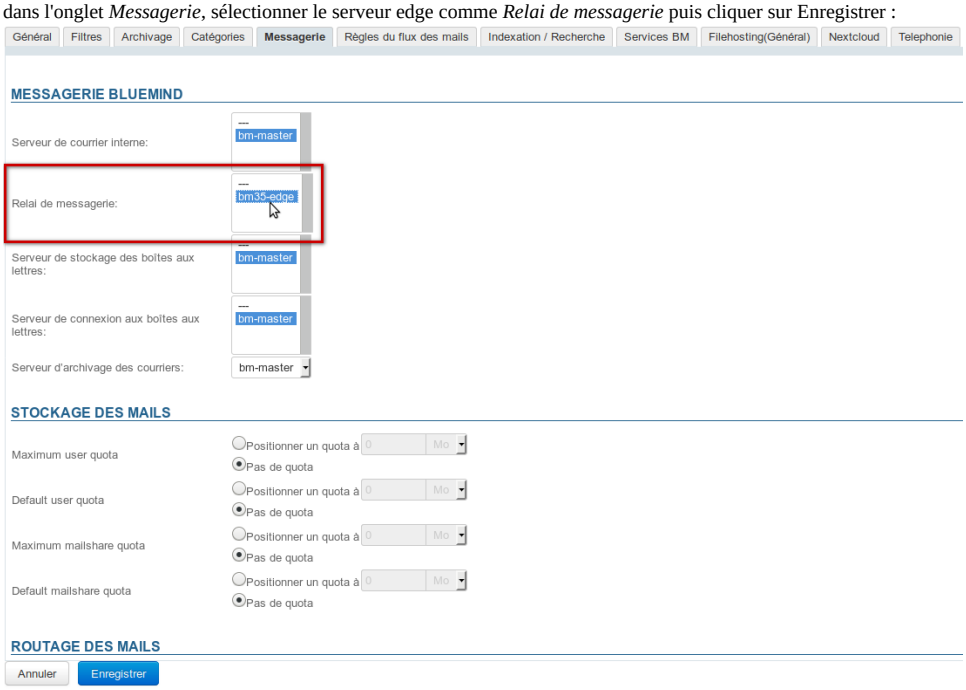


- dans la liste des serveurs, le serveur edge apparaît bien avec le tag lié au relai de messagerie *mail/smtp-edge*

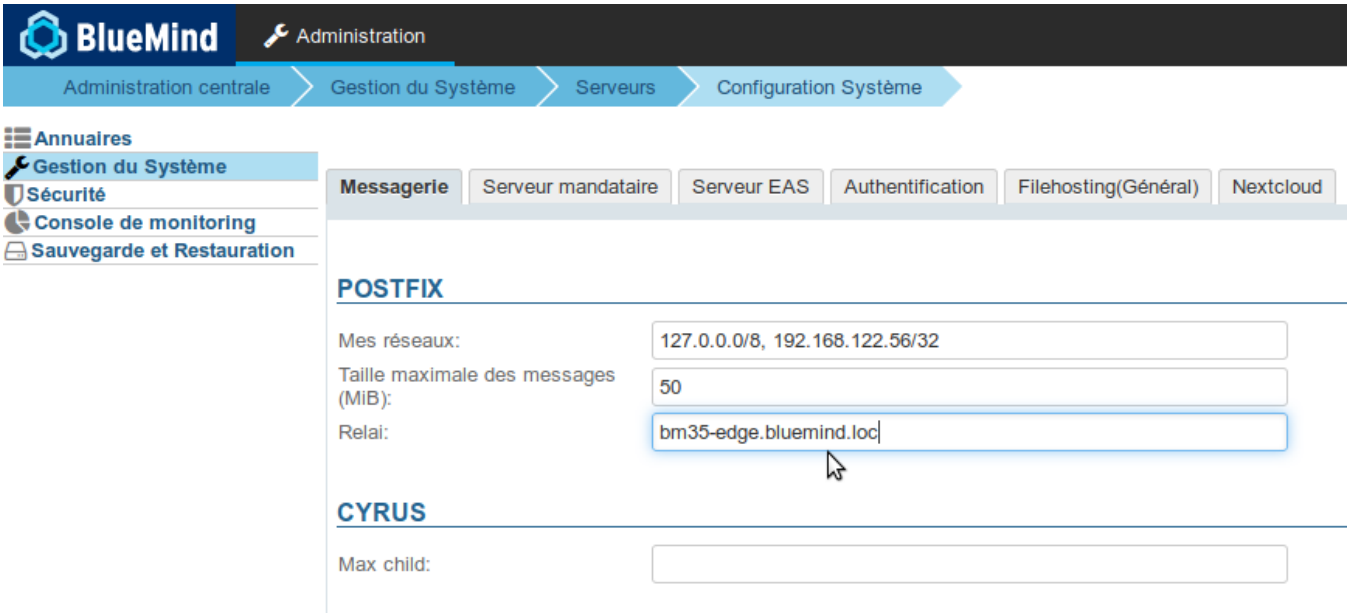


5. configurer le domaine pour utiliser ce serveur comme relai de messagerie

- toujours en tant qu'utilisateur admin0@global.virt, naviguer dans *Gestion du Système* > *Domaines supervisés*
- cliquer sur la ligne correspondant au domaine à configurer
- dans l'onglet *Messagerie*, sélectionner le serveur edge comme *Relai de messagerie* puis cliquer sur Enregistrer :



6. configurer le serveur pour envoyer les mails sortant à travers le relai :
   - toujours en tant que l'utilisateur admin0@global.virt, naviguer dans *Gestion du Système* > *Configuration Système*
   - dans l'onglet *Messagerie*, remplir le champ *Relai* avec l'adresse IP ou le nom d'hôte du serveur edge puis cliquer sur Enregistrer :



NGINX

Configuration de l'accès web

1. Se connecter en tant que root sur le serveur edge
2. naviguer jusqu'au dossier `/etc/nginx/sites-available`

```
bm35-edge.bluemind.loc:~# cd /etc/nginx/sites-available
```

3. créer un fichier de configuration `bm-proxy` et l'éditer, par exemple avec vim :

```
bm35-edge.bluemind.loc:/etc/nginx/sites-available# vim bm-proxy
```

4. ajouter les lignes suivantes :

```
server {
  listen 80;
  # <url_externe_bluemind> désigne l'url externe à laquelle les utilisateurs se connectent
  server_name <url_externe_bluemind>;

  location / {
        return 301 https://<url_externe_bluemind>$request_uri;
  }
}

server {
  listen 443 ssl;
  server_name <url_externe_bluemind>;

  ssl_certificate /etc/ssl/certs/bm_cert.pem;
  ssl_certificate_key /etc/ssl/certs/bm_cert.pem;
  ssl_session_timeout 5m;
  ssl_prefer_server_ciphers on;

  ssl_protocols TLSv1.2;
  ssl_ciphers 'EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:EECDH+aRSA+SHA384:EECDH+aRSA+SHA256:
EECDH:+CAMELLIA256:+AES256:+CAMELLIA128:+AES128:+SSLv3:!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!
PSK:!DSS:!RC4:!SEED:!ECDSA:CAMELLIA256-SHA:AES256-SHA:CAMELLIA128-SHA:AES128-SHA';
  add_header Strict-Transport-Security max-age=15768000; # six months

 proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;

 location / {
        # <srv_interne> est le serveur BlueMind principal
    proxy_pass https://<srv_interne>;
  }

  location /webmail/ {
    client_max_body_size 0m;
    proxy_pass https://<srv_interne>/webmail/;
  }

  location /Microsoft-Server-ActiveSync {
    proxy_pass https://<srv_interne>/Microsoft-Server-ActiveSync;
    proxy_read_timeout 1200s;
    proxy_headers_hash_bucket_size 128;
    proxy_headers_hash_max_size 2048;
    client_max_body_size 0m;
    proxy_pass_header Server;
  }

  location /eventbus {
    proxy_pass https://<srv_interne>;
    proxy_http_version 1.1;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection "upgrade";
  }

  location /api/filehosting/ {
    client_max_body_size 0m;
    proxy_pass https://<srv_interne>$request_uri;
    proxy_set_header        X-Real-IP       $remote_addr;
    proxy_set_header        X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_http_version 1.1;
    proxy_buffering off;
  }

  location /api/attachment/ {
    client_max_body_size 0m;
```

```
    proxy_pass https://<srv_interne>$request_uri;
    proxy_set_header        X-Real-IP       $remote_addr;
    proxy_set_header        X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_http_version 1.1;
    proxy_buffering off;
  }

  location /fh/ {
    proxy_pass https://<srv_interne>/fh/;
    proxy_http_version 1.1;
    proxy_buffering off;
  }
}
```

5. sauvegarder le fichier et quitter l'éditeur
6. exécuter les commandes suivantes pour mettre en place la configuration :

```
bm35-edge.bluemind.loc:/etc/nginx/sites-available# ln -s /etc/nginx/sites-available/bm-proxy
/etc/nginx/sites-enabled/
bm35-edge.bluemind.loc:/etc/nginx/sites-available# rm /etc/nginx/sites-enabled/default
```

7. recharger la configuration du serveur nginx :

BlueMind 3.5.x BlueMind 3.0.x

```
bm35-edge.bluemind.loc:/etc/nginx/sites-available# service bm-nginx reload
```

```
bm35-edge.bluemind.loc:/etc/nginx/sites-available# service nginx reload
```

Configuration de la messagerie

1. Sur le serveur edge, copier le fichier de configuration du serveur principal situé à l'emplacement `/etc/nginx/global.d/bm-proxy-mail.conf`. Il est possible pour cela d'utiliser scp :

```
bm35-edge.bluemind.loc:~# scp root@srv1.bluemind.loc:/etc/nginx/global.d/bm-mail-proxy.conf
/etc/nginx/global.d/
```

2. éditer le fichier `/etc/nginx/global.d/bm-mail-proxy.conf` sur le serveur edge et remplacer l'adresse IP de la ligne `auth_http` par l'adresse IP du serveur principal
3. recharger la configuration nginx :

BlueMind 3.5.x BlueMind 3.0.x

```
bm35-edge.bluemind.loc:~# service bm-nginx reload
```

```
bm35-edge.bluemind.loc:~# service nginx reload
```

Configuration XMPP

Pour que le serveur prenne en charge la gestion du flux XMPP :

1. créer le fichier `/etc/nginx/global.d/bm-xmpp-proxy.conf` avec le contenu suivant :

```
stream {
    upstream backend_xmpp {
        least_conn;

                server 1.2.3.4:5222;
                server 1.2.3.5:5222 backup;
    }

    server {
        listen 5222;
        proxy_pass backend_xmpp ;
    }
}
```

en remplaçant 1.2.3.4 par l'adresse IP du serveur principal, ou du serveur ayant le rôle XMPP s'il y a lieu

2. Recharger la configuration nginx :

BlueMind 3.5.x BlueMind 3.0.x

```
bm35-edge.bluemind.loc:~# service bm-nginx reload
```

```
bm35-edge.bluemind.loc:~# service nginx reload
```

PROXY APACHE

Il est aussi possible d'utiliser Apache comme proxy à la place de Nginx. Pour cela, il faudra utiliser une version >=2.4 d'Apache et activer les modules suivant :

- mod_ssl
- mod_proxy et mod_proxy_wstunnel
- mod_rewrite

Exemple de VirtualHost pour Apache :

```
<VirtualHost *:80>
        Redirect / https://<url_externe_bluemind>/
</VirtualHost>

<VirtualHost *:443>
        SSLEngine On

        SSLCertificateFile     "/etc/ssl/certs/bm_cert.pem"
        SSLCertificateKeyFile  "/etc/ssl/certs/bm_cert.pem"

        SSLProxyEngine On
        SSLProxyCheckPeerCN Off
        SSLProxyCheckPeerName Off
        SSLProxyVerify none

        # Websocket proxy
        RewriteEngine on
        RewriteCond %{HTTP:UPGRADE} ^WebSocket$ [NC]
        RewriteCond %{HTTP:CONNECTION} Upgrade$ [NC]
        RewriteRule .* wss://<srv_interne>%{REQUEST_URI} [P]

        ProxyPreserveHost On
        <Location />
                ProxyPass https://<srv_interne>/
                ProxyPassReverse https://<srv_interne>/
        </Location>
</VirtualHost>
```