

# Configuration fonctionnelle Zimbra OSS 7.0.1 avec Z-Push

## Configuration générale

Toutes les machines sont des serveurs debian 5 virtualisés avec OpenVZ. L'infrastructure du réseau est la suivante :

Internet ->Routeur FAI->Firewall 1->DMZ->Firewall 2->réseau local

Les domaines sont domaine.fr et domaine.local.

- Le serveur Zimbra est zimbra.domaine.fr et est sur le réseau local.
- Le serveur Z-push est synchro.domaine.fr et est sur le réseau local.

Nous possédons une plage de 6 adresses IP publiques. Les DNS de notre fournisseur d'accès sont configurés afin de diriger zimbra.domaine.fr vers notre ip publique 1 et synchro.domaine.fr vers notre ip publique 2.

## Configuration de la DMZ

Dans la DMZ, nous disposons de deux serveurs apache2 configurés en reverse proxy : proxy1.domaine.local, proxy2.domaine.local.

Le firewall 1 redirige les requêtes http/https pour zimbra.domaine.fr vers proxy1 et les requêtes http/https pour synchro.domaine.fr vers proxy2.

La configuration du proxy 1 est la suivante : /etc/apache2/sites-enabled/server

```
<VirtualHost *:443>
  ServerName proxy1.domaine.local
  SSLEngine on
  SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
  SSLCertificateFile /etc/apache2/ssl/ippublique1.crt
  SSLCertificateKeyFile /etc/apache2/ssl/ippublique1.key
  SSLProxyEngine on
  SSLProxyCACertificateFile /etc/apache2/ssl/AC.domaine.local.crt

  RequestHeader set Front-End-Https On
  ProxyRequests On
  ProxyPreserveHost On
  ProxyVia full

  <Proxy *>
    Order deny,allow
    Allow from all
  </Proxy>

  ProxyPass          / https://zimbra.domaine.fr/
  ProxyPassReverse   / https://zimbra.domaine.fr/
</VirtualHost>

<VirtualHost *:80>
  ServerName proxy1.domaine.local
  <IfModule mod_rewrite.c>
    RewriteEngine on
    RewriteCond %{HTTPS} off
    RewriteRule (.*?) https://%{HTTP_HOST}%{REQUEST_URI}
  </IfModule>

  ProxyRequests On
  ProxyPreserveHost On
  ProxyVia full

  <Proxy *>
    Order deny,allow
    Allow from all
  </Proxy>

  Redirect permanent / https://proxy1.domaine.local/
</VirtualHost>
```

La configuration du proxy 2 est la suivante : /etc/apache2/sites-enabled/server

```
<VirtualHost *:443>
    ServerName proxy2.domaine.local
    SSLEngine on
    SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
    SSLCertificateFile /etc/apache2/ssl/ippublique2.crt
    SSLCertificateKeyFile /etc/apache2/ssl/ippublique2.key
    SSLProxyEngine on
    SSLProxyCACertificateFile /etc/apache2/ssl/AC.domaine.local.crt

    RequestHeader set Front-End-Https On
    ProxyRequests On
    ProxyPreserveHost On
    ProxyVia full

    <Proxy *>
        Order deny,allow
        Allow from all
    </Proxy>

    ProxyPass          / https://synchro.domaine.fr/
    ProxyPassReverse   / https://synchro.domaine.fr/
</VirtualHost>

<VirtualHost *:80>
    ServerName proxy2.domaine.local

    ProxyRequests On
    ProxyPreserveHost On
    ProxyVia full

    <Proxy *>
        Order deny,allow
        Allow from all
    </Proxy>

    ProxyPass          / http://synchro.domaine.fr/
    ProxyPassReverse   / http://synchro.domaine.fr/
</VirtualHost>
```

Pour la configuration de la DMZ, mises à part les règles de sécurisation des flux sur les deux firewalls, il n'y a rien de plus.

- Le firewall 1 autorise uniquement le trafic http/https vers proxy1 et proxy2.
- Le firewall 2 autorise uniquement le trafic entre proxy1 et zimbra.domaine.fr et proxy2 et synchro.domaine.fr.

Les deux serveurs de la DMZ ont comme passerelle par défaut le firewall 1 et comme DNS les DNS internes dns1.domaine.local et dns2.domaine.local.

La machine hôte a dans son fichier /etc/network/interfaces, la route statique :  
up route add -net reseau local/24 gw firewall2 dev eth0

Ainsi, les proxy de la DMZ "connaissent" synchro.domaine.fr et zimbra.domaine.fr par leurs ip locales et non publiques.

### **Configuration du réseau local**

Les serveurs DNS de l'AD (windows server 2003 R2) sont configurés avec deux zones DNS : domaine.local et domaine.fr.

La zone domaine.local contient tous les ordinateurs et serveurs y compris notre autorité de certification interne : AC.domaine.local.

La zone domaine.fr ne contient que les enregistrements :

- MX : le serveur SMTP de notre FAI : smtp.fai.org
- MX : le serveur zimbra.domaine.fr
- Hôte : zimbra.domaine.fr
- Hôte : synchro.domaine.fr

Ainsi, pour les utilisateurs "nomades", lorsqu'ils sont connectés au réseau, les serveurs DNS internes leur permettent d'accéder aux serveurs zimbra et synchro par l'adresse ip interne et lorsqu'ils se connectent à distance, les DNS externes leur permettent de se connecter via les ip publiques.

## Configuration du serveur Zimbra

Le serveur Zimbra est en mode **https** strict. En interne, ce n'est pas utile mais pour les accès externes , ça l'est. Du coup pour qu'il n'y ait pas d'erreur lors de l'accès aux documents partagés par exemple, cela devient nécessaire.

Bon et puis c'est comme ça épécétout ;D.

Les points clés de la configuration Zimbra sont les suivants :

Authentification SMTP (le SMTP de notre FAI exige une authentification pour envoyer des mails à l'extérieur du domaine d'où la création d'un user zimbrauser pour envoyer les mails) :

```
1. Vérifier la présence du fichier /opt/zimbra/conf/relay_password sinon exécuter la commandes:  
echo smtp.fai.org zimbrauser:zimbrapassword > /opt/zimbra/conf/relay_password
```

```
2. Autoriser zimbra à envoyer des mails depuis smtp.fai.org  
su - zimbra  
zmprov ms zimbra.domaine.fr zimbraMtaRelayHost smtp.fai.org  
postmap hash:/opt/zimbra/conf/relay_password  
postconf -e smtp_sasl_password_maps=hash:/opt/zimbra/conf/relay_password  
postconf -e smtp_sasl_auth_enable=yes  
postconf -e smtp_cname_overrides_servername=no  
postconf -e smtp_sasl_security_options=noanonymous  
postfix reload  
  
zmlocalconfig -e postfix_smtp_sasl_password_maps=hash:/opt/zimbra/conf/relay_password  
zmlocalconfig -e postfix_smtp_sasl_security_options=noanonymous  
zmlocalconfig -e postfix_smtp_cname_overrides_servername=no  
zmcontrol restart
```

Envoi des mails aux adresses domaine.fr non installées sur le serveur (nécessaire lors de la migration) :

```
zmprov md domaine.fr zimbraMailCatchAllAddress @domaine.fr  
zmprov md domaine.fr zimbraMailCatchAllForwardingAddress @domaine.fr  
zmprov md domaine.fr zimbraMailTransport smtp:smtp.fai.org  
zmprov mcf zimbraMtaRelayHost smtp.fai.org  
zmprov mcf zimbraMtaDnsLookupsEnabled FALSE
```

HTTPS :

```
zmprov md domaine.fr zimbraPublicServiceHostname zimbra.domaine.fr  
zmprov md domaine.fr zimbraPublicServiceProtocol https  
zmprov md domaine.fr zimbraPublicServicePort 443
```

Toutes ces jolies choses ont été trouvées en fouillant dans le forum zimbrafr (un grand merci à tous et en particulier à Klug et Bartounet) et sur le wiki.

## Configuration du Push

Je me suis basé sur les travaux de Guillaume POMENTE :

Post : [http://www.zimbrafr.org/forum/topic/3171-z-push/page\\_p\\_22576\\_hl\\_z-push\\_fromsearch\\_1#entry22576](http://www.zimbrafr.org/forum/topic/3171-z-push/page_p_22576_hl_z-push_fromsearch_1#entry22576)

Blog : <http://www.guillaume-p.net/tutorial-howto-installation-configuration-z-push-zimbra-open-source/>

Sur la machine appelé synchro.domaine.fr, j'ai installé apache2, php5 et php-curl. J'ai ensuite téléchargé la dernière version de z-push : <http://prdownload.berlios.de/z-push/z-push-1.5.1.tar.gz>.

J'ai téléchargé la dernière version du backend Zimbra :

<http://sourceforge.net/projects/zimbrabackend/files/Release48/zimbra48.tgz/download>.

J'ai fait les modifications de droits :

```
chmod 755 /var/www/z-push/state  
chown www-data:www-data /var/www/z-push/state
```

Le fichier zimbra.php contenu dans l'archive du Zimbra Backend doit être décompressé dans /var/www/z-push/backend.

La synchronisation se fait via SSL, voici mes fichiers de configuration :

/etc/apache2/sites-enabled/server

```
<VirtualHost *:80>
    ServerName synchro.domaine.fr

    DocumentRoot /var/www/calendar/
    <Directory />
        Options FollowSymLinks
        AllowOverride None
    </Directory>
    <Directory /var/www/calendar/>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride None
        Order allow,deny
        allow from all
    </Directory>

    ErrorLog /var/log/apache2/error.log
    LogLevel warn
    CustomLog /var/log/apache2/access.log combined

    Alias /doc/ "/usr/share/doc/"
    <Directory "/usr/share/doc/">
        Options Indexes MultiViews FollowSymLinks
        AllowOverride None
        Order deny,allow
        Deny from all
        Allow from 127.0.0.0/255.0.0.0 ::1/128
    </Directory>
</VirtualHost>

<VirtualHost *:443>
    ServerName synchro.domaine.fr

    DocumentRoot /var/www/z-push/

    <Directory />
        Options FollowSymLinks
        AllowOverride None
    </Directory>
    <Directory /var/www/z-push/>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride None
        Order allow,deny
        allow from all
    </Directory>

    ErrorLog /var/log/apache2/error.log
    LogLevel warn
    CustomLog /var/log/apache2/ssl_access.log combined

    Alias /doc/ "/usr/share/doc/"
    <Directory "/usr/share/doc/">
        Options Indexes MultiViews FollowSymLinks
        AllowOverride None
        Order deny,allow
        Deny from all
        Allow from 127.0.0.0/255.0.0.0 ::1/128
    </Directory>

    Alias /Microsoft-Server-ActiveSync /var/www/z-push/index.php

    php_flag magic_quotes_gpc off
    php_flag register_globals off
    php_flag magic_quotes_runtime off
    php_flag short_open_tag on

    SSLEngine on
    SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
    SSLCertificateFile /etc/apache2/ssl/synchro.domaine.fr.crt
    SSLCertificateKeyFile /etc/apache2/ssl/private/synchro.domaine.fr.key
```

```
SSLProxyCACertificateFile /etc/apache2/ssl/CA/AC.domaine.local
```

```
<FilesMatch "\.(cgi|shtml|phtml|php)$">
    SSLOptions +StdEnvVars
</FilesMatch>
```

```
BrowserMatch ".*MSIE.*" \
    nokeepalive ssl-unclean-shutdown \
    downgrade-1.0 force-response-1.0
```

```
</VirtualHost>
```

## /var/www/z-push/config.php

```
<?php
/*****
* File      :   config.php
* Project   :   Z-Push
* Descr     :   Main configuration file
*
* Created    :   01.10.2007
*
* Copyright 2007 - 2010 Zarafa Deutschland GmbH
*
* This program is free software: you can redistribute it and/or modify
* it under the terms of the GNU Affero General Public License, version 3,
* as published by the Free Software Foundation with the following additional
* term according to sec. 7:
*
* According to sec. 7 of the GNU Affero General Public License, version 3,
* the terms of the AGPL are supplemented with the following terms:
*
* "Zarafa" is a registered trademark of Zarafa B.V.
* "Z-Push" is a registered trademark of Zarafa Deutschland GmbH
* The licensing of the Program under the AGPL does not imply a trademark license.
* Therefore any rights, title and interest in our trademarks remain entirely with us.
*
* However, if you propagate an unmodified version of the Program you are
* allowed to use the term "Z-Push" to indicate that you distribute the Program.
* Furthermore you may use our trademarks where it is necessary to indicate
* the intended purpose of a product or service provided you use it in accordance
* with honest practices in industrial or commercial matters.
* If you want to propagate modified versions of the Program under the name "Z-Push",
* you may only do so if you have a written permission by Zarafa Deutschland GmbH
* (to acquire a permission please contact Zarafa at trademark@zarafa.com).
*
* This program is distributed in the hope that it will be useful,
* but WITHOUT ANY WARRANTY; without even the implied warranty of
* MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
* GNU Affero General Public License for more details.
*
* You should have received a copy of the GNU Affero General Public License
* along with this program. If not, see <http://www.gnu.org/licenses/>.
*
* Consult LICENSE file for details
*****/
// Defines the default time zone
if (function_exists("date_default_timezone_set")){
    date_default_timezone_set("Europe/Paris");
}

// Defines the base path on the server, terminated by a slash
define('BASE_PATH', dirname($_SERVER['SCRIPT_FILENAME']) . "/");
```

```
// Define the include paths
ini_set('include_path',
        BASE_PATH. "include/" . PATH_SEPARATOR .
        BASE_PATH. PATH_SEPARATOR .
        ini_get('include_path') . PATH_SEPARATOR .
        "/usr/share/php/" . PATH_SEPARATOR .
        "/usr/share/php5/" . PATH_SEPARATOR .
        "/usr/share/pear/");

define('STATE_DIR', BASE_PATH. '/state');

// Try to set unlimited timeout
define('SCRIPT_TIMEOUT', 0);

//Max size of attachments to display inline. Default is 1MB
define('MAX_EMBEDDED_SIZE', 1048576);

// Device Provisioning
define('PROVISIONING', false);

// This option allows the 'loose enforcement' of the provisioning policies for older
// devices which don't support provisioning (like WM 5 and HTC Android Mail) - dw2412
contribution
// false (default) - Enforce provisioning for all devices
// true - allow older devices, but enforce policies on devices which support it
define('LOOSE_PROVISIONING', false);

// Default conflict preference
// Some devices allow to set if the server or PIM (mobile)
// should win in case of a synchronization conflict
// SYNC_CONFLICT_OVERWRITE_SERVER - Server is overwritten, PIM wins
// SYNC_CONFLICT_OVERWRITE_PIM - PIM is overwritten, Server wins (default)
define('SYNC_CONFLICT_DEFAULT', SYNC_CONFLICT_OVERWRITE_PIM);

// The data providers that we are using (see configuration below)
// $BACKEND_PROVIDER = "BackendICS";
$BACKEND_PROVIDER = "BackendZimbra";

// *****
// BackendICS settings
// *****

// Defines the server to which we want to connect
define('MAPI_SERVER', 'file:///var/run/zarafa');
define('ZIMBRA_URL', 'https://zimbra.domaine.fr');
define('ZIMBRA_USER_DIR', 'zimbra');
define('ZIMBRA_SYNC_CONTACT_PICTURES', true);
define('ZIMBRA_VIRTUAL_CONTACTS', true);
define('ZIMBRA_VIRTUAL_APPOINTMENTS', true);
define('ZIMBRA_VIRTUAL_TASKS', true);
define('ZIMBRA_IGNORE EMAILED_CONTACTS', true);
define('ZIMBRA_HTML', false);
define('IMAP_DEFAULTFROM', '');
define('IMAP_SENTFOLDER', '');

// *****
// BackendMaildir settings
// *****
define('MAILDIR_BASE', '/tmp');
define('MAILDIR_SUBDIR', 'Maildir');

// *****
// BackendVCDIR settings
// *****
define('VCARD_DIR', '/home/%u/.kde/share/apps/kabc/stdvcf');

// Alternative backend to perform SEARCH requests (GAL search)
// if an empty value is used, the default search functionality of the main backend is used
// use 'SearchLDAP' to search in a LDAP directory (see backend/searchldap/config.php)
define('SEARCH_PROVIDER', '');

?>
```

## Configuration pour partager l'agenda Zimbra dans un agenda Gmail

J'ai suivi les travaux de John Lewis :

Post : <http://www.zimbra.com/forums/administrators/5074-syncing-zimbra-google-calendar-4.html>

Site : <http://www.unicon.net/node/1300>

Il est vrai que pour le boulot, ça ne me sert à rien, en revanche, comme l'explique Jean-Louis dans son article (je traduis) : ma famille utilise Google Calendar et je voudrais que ma femme puisse voir mon agenda pro. Et souvenez-vous que Google ne sait pas se synchroniser avec un calendrier https !

J'ai donc suivi son tutoriel extrêmement simple.

La première étape consiste à partager dans Zimbra son calendrier avec un Utilisateur. Pour cela, il faut fournir l'adresse mail de l'utilisateur (par exemple : [mafemme@gmail.com](mailto:mafemme@gmail.com)) et créer un mot de passe pour l'accès au calendrier.

Ensuite, sur un serveur interne, ici intranet.domaine.local, qui n'est pas accessible de l'extérieur, on installe le script php : calendarurl.php

```
<html>
<head>
<title>Private Calendar Share URL</title>
</head>
<body>
<h1>Private Calendar Share URL</h1>
<?php

$key = '12345678123456781234567812345678';
$iv = '12345678' ;
$calurl = 'http://synchro.domaine.fr/calendar.php';

if (isset($_POST['submit'])) {
    $login = $_POST['login'];
    $password = $_POST['password'];
    $user = $_POST['user'];
    $calendar = $_POST['calendar'];
    $daysback = $_POST['daysback'];
    $daysforward = $_POST['daysforward'];
    $input = implode('|', array($login, $password, $user, $calendar, $daysback, $daysforward));
    $input = crc32($input)."|".$input;
    $cipher = mcrypt_module_open(MCRYPT_BLOWFISH, '', MCRYPT_MODE_CBC, '');
    mcrypt_generic_init($cipher, $key, $iv);
    $id = strtr(base64_encode(mcrypt_generic($cipher, $input)), '+/=', '-_');
    mcrypt_generic_deinit($cipher);
    mcrypt_module_close($cipher);
    $url = $calurl.'?id='.$id;
    echo '<a href="'.$url.'">'.$url.'</a>';
} else {
    ?>
    <form method="post" action="<?php echo $PHP_SELF;?>">
    <table>
    <tr><th>Login</th><td><input type="text" size="20" name="login" />
    (Guest email address for which the calendar share was created)</td></tr>
    <tr><th>Password</th><td><input type="text" size="20" name="password" />
    (Password from the guest calendar share)</td></tr>
    <tr><th>User</th><td><input type="text" size="20" name="user" />
    (Username of the account being shared)</td></tr>
    <tr><th>Calendar</th><td><input type="text" size="20" name="calendar" value="Calendar" />
    (Name of calendar being shared)</td></tr>
    <tr><th>Days Back</th><td><input type="text" size="20" name="daysback" value="30" />
    (Number of days in the past the iCal feed should include)</td></tr>
    <tr><th>Days Forward</th><td><input type="text" size="20" name="daysforward" value="90" />
    (Number of days in the future the iCal feed should include)</td></tr>
    <tr><th colspan="2"><input type="submit" value="Submit" name="submit" /></th></tr>
    </table>
    </form>
    <?php
    }
    ?>
</body>
</html>
```

Ce script affiche un formulaire qui permet de générer une URL de la mort qui sera celle à ajouter à l'agenda gmail, du type :

<http://synchro.domaine.fr/calendar.php?id=Y-eR1-c6xsNzB49fvsJKkrD0DOtLMIV7Pcs6GdrvYHqdgUjxE3DhZuZb78g6B2FMRGmkZ9UFY9DwQwKRu5fCQ,,>

# Private Calendar Share URL

<b>Login</b>	<input type="text" value="mafemme@gmail.com"/>	(Guest email address for which the calendar share was created)
<b>Password</b>	<input type="text" value="motdepasse"/>	(Password from the guest calendar share)
<b>User</b>	<input type="text" value="monusernameZimbra"/>	(Username of the account being shared)
<b>Calendar</b>	<input type="text" value="Calendar"/>	(Name of calendar being shared)
<b>Days Back</b>	<input type="text" value="30"/>	(Number of days in the past the iCal feed should include)
<b>Days Forward</b>	<input type="text" value="90"/>	(Number of days in the future the iCal feed should include)
<input type="button" value="Submit"/>		

Sur le serveur synchro.domaine.fr, j'ai copié le script calendar.php :

```
<?php
$key = '12345678123456781234567812345678';
$iv = '12345678' ;

$id = $_GET['id'];

$result = 'HTTP/1.1 400 Bad Request';

if (isset($id)) {
    $cipher = mcrypt_module_open(MCRYPT_BLOWFISH, '', MCRYPT_MODE_CBC, '');
    mcrypt_generic_init($cipher, $key, $iv);
    $id = rtrim(mdecrypt_generic($cipher, base64_decode(strtr($id, '-_', '+/'))), "\0");
    mcrypt_generic_deinit($cipher);
    mcrypt_module_close($cipher);
    list($crc, $id) = explode("|", $id, 2);
    if (is_numeric($crc) && (!empty($id)) && ($crc == crc32($id))) {
        list($login, $password, $user, $calendar, $daysback, $daysforward) = explode("|",
$id);

        $url = "https://".urlencode($login).":".urlencode($password).
            "@zimbra.domaine.fr/home/".urlencode($user)."@domaine.fr/".
            urlencode($calendar)."?fmt=ics&start=-".$daysback."d&end="
$daysforward."d";
        $calendar = @file_get_contents($url);
        $result = $http_response_header[0];
        if ($result == 'HTTP/1.1 200 OK') {
            header('Content-Type: text/calendar; charset=utf-8');
            header('Content-Disposition: attachment; filename="calendar.ics"');
            print $calendar;
            exit();
        }
    }
}
header($result);
?>
<html>
<body>
<h1><?php echo $result; ?></h1>
</body>
</html>
```

Chez moi, cela fonctionne parfaitement.