Activation de l’authentification LDAP

Ce document décrit la configuration à mettre en oeuvre afin d’activer l’authentification LDAP sur un serveur Mapping ONYX.

Ce mode d’authentification permet aux utilisateurs de se connecter à l’interface Web du serveur Mapping ONYX en utilisant le même identifiant et le même mot de passe que sur Windows ou sur les applications “métier”.

Principe

Pour des raisons de sécurité, la configuration LDAP doit se faire exclusivement côté serveur web Apache.

Cette méthode nécessite d’ajouter manuellement au référentiel Mapping les utilisateurs ayant besoin d’un accès à l’interface Web, afin de leur accorder les autorisations d’accès aux fonctionnalités dont ils ont besoin.

Pré-requis

– Serveur Apache version 2.4

– Le module apache **mod_ldap** doit être installé et activéExemple : yum install mod_ldap (sur Centos ou Redhat)

– Un annuaire LDAP (Active Directory, OpenLdap…) doit être accessible du serveur Mapping et sa configuration connue :- Adresse IP ou DNS du serveur- Utilisateur ayant accès en lecture à l’annuaire (bind)

Configuration côté Apache

Le type d’authentification par défaut à l’installation de Mapping est basé sur un fichier texte contenant la liste des utilisateurs et leur mot de passe (AuthBasicProvider file) : c’est le fichier .htpasswd, qui est présent à la racine du dossier MapHTTPServer.

La configuration qui suit décrit les modifications à apporter à la configuration Apache afin de remplacer cette authentification “fichier” par une authentification “ldap”.

D’autre part, le serveur Mapping est historiquement installé avec une configuration web basée sur la présence d’un fichier “.htaccess”. L’utilisation d’un tel fichier n’étant pas conseillée, toute la configuration devra être réalisée directement dans le fichier httpd.conf (ou l’un des sous-fichiers de configuration présents dans le dossier conf.modules.d le cas échéant).

Modification du fichier httpd.conf

1. Si ce n’est pas déjà le cas, simplifier la configuration “Mapping” de ce

fichier comme suit :- Supprimer le noeud <Directory /xxxxx/xxxxx/MapHTTPServer/cgi-bin> (le noeud xml complet avec tout son contenu et la balise de fin </Directory>)- Supprimer AllowOverride all : afin de ne plus autoriser l'utilisation de fichiers .htaccess- Supprimer Order allow,deny : instruction non compatible avec Apache 2.4- Supprimer Allow from all : instruction non compatible avec Apache 2.4

2. Ajouter ou adapter les instructions suivantes permettant l'authentification LDAP- **AuthType Basic**– **AuthName Identification**– **AuthBasicProvider ldap** : activation de l'authentification LDAP- **AuthLDAPBindDN** : DN complet de l'utilisateur utilisé pour accéder à l'annuaire LDAP en lecture- **AuthLDAPBindPassword** : mot de passe de cet utilisateur- **AuthLDAPURL** : URL du serveur LDAP, emplacement racine des utilisateurs et filtre de recherche- **LDAPReferrals off** : Désactivation des redirections vers les serveurs LDAP alternatifs- **Require valid-user** : Permet de laisser passer uniquement les utilisateurs pouvant s'authentifierPour plus d'information, une documentation détaillée sur l'authentification LDAP sous Apache est disponible à l'emplacement suivant : https://httpd.apache.org/docs/current/fr/mod/mod_authnz_ldap.html
3. Supprimer (ou renommer) le fichier MapHTTPServer/.htaccess dans l'arborescence Mapping*Exemple : /apps/mapping/MapHTTPServer/.htaccess ou c:\Mapping\M-Processing Server\MapHTTPServer\.htaccess*

Exemple de configuration dans le fichier httpd.conf

```
#BEGIN_MAPPING_v9.0xxxxx
#DO NOT MODIFY THIS BLOCK. It will be automatically updated.
Listen 8002
&lt;VirtualHost *:8002&gt;
        ServerName 127.0.0.1
        DocumentRoot "C:/MAPPING/M-ProcessingServer/MapHTTPServer"
        ScriptAlias /cgi-bin/ "C:/MAPPING/M-
ProcessingServer/MapHTTPServer/cgi-bin/"
        &lt;Directory "C:/MAPPING/M-ProcessingServer/MapHTTPServer"&gt;
              AuthType Basic
              AuthName Identification
              <strong>AuthBasicProvider ldap</strong>
              <strong>AuthLDAPBindDN "CN=Jacques Dewael, OU=Current,
OU=Mapping, DC=mapping400, DC=local"</strong>
              <strong>AuthLDAPBindPassword "a54G$2!="</strong>
              <strong>AuthLDAPURL
"ldap://192.168.1.5/dc=mapping,dc=local?sAMAccountName?sub?(objectClass=perso
n)"</strong>
              <strong>LDAPReferrals Off</strong>
              <strong>Require valid-user</strong>
              Options None
        &lt;/Directory&gt;
&lt;/VirtualHost&gt;
#END_MAPPING_v9.0.xxxxx
```

Restriction sur les plateformes Linux et AIX – Pour des raisons de compatibilité avec l'interface de Workflow, il n'est pas possible à ce jour, sur les plateformes Linux et AIX, de se connecter avec le "userPrincipalName" (identifiant du type **user@domain.xxx**). Cette restriction sera levée dans une version ultérieure.

Configuration côté Mapping

L'administrateur

L'utilisateur "administrateur" du serveur Mapping est spécifié dans le fichier de configuration "mapping.conf", via le paramètre "USER_ADMIN". Par défaut, sa valeur est "mapadmin".

Cela implique donc *(au choix)* :- De créer un utilisateur "mapadmin" dans l'annuaire ldap *(seule solution à ce jour sur plateformes Linux et AIX)*– Ou de modifier la valeur du paramètre "USER_ADMIN" afin d'y renseigner l'identifiant d'un utilisateur de l'annuaire ldap déjà existant ou créé spécialement pour cet usage.

Les autres utilisateurs

Les autres utilisateurs ayant besoin de se connecter à l'interface Web du serveur Mapping doivent être créés au préalable depuis l'interface d'administration Mapping et affectés à leurs groupes respectifs :Cf. Documentation sur la gestion des utilisateurs et droits d'accès

Les mots de passe renseignés lors de la création de ces utilisateurs ne sont pas exploités dans le cadre d'une authentification LDAP.

Les utilisateurs se connectant sans avoir été référencés au préalable se retrouveront devant une page web vide.