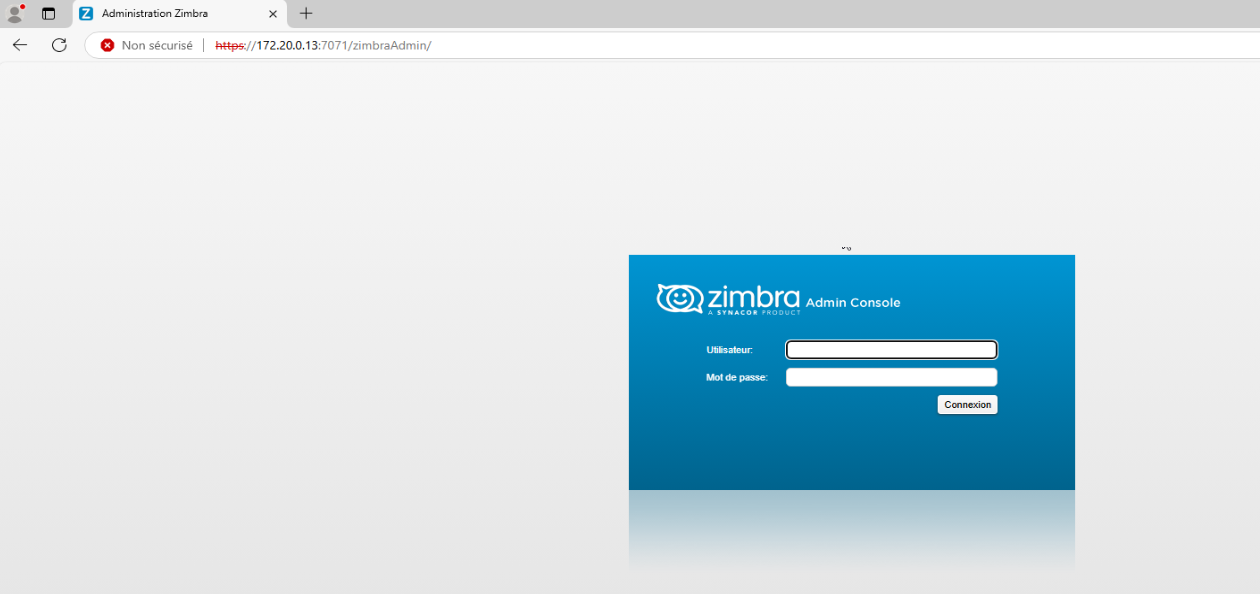
**Mise en Place de la Liaison LDAP entre Zimbra et Active Directory**

L’objectif est de configurer Zimbra pour utiliser Active Directory (AD) comme source d’authentification via le protocole LDAP.

**Étape 1 : Accès à l’interface d’administration de Zimbra**

Ouvrez un navigateur et accédez à l’interface d’administration via l’URL suivante :  
https://172.20.0.13:7071/

Connectez-vous avec un compte administrateur Zimbra.

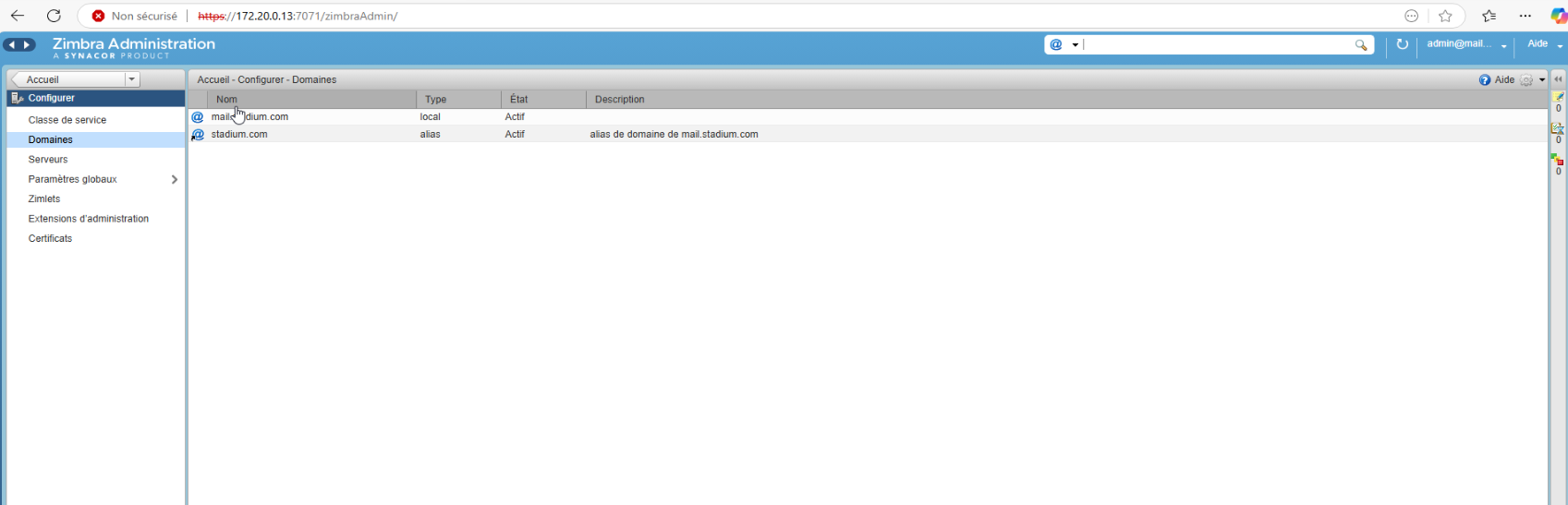


**Étape 2 : Accéder aux Paramètres d’Authentification Externe**

Dans le tableau de bord Zimbra, cliquez sur "Configuration".

Cliquez sur "Domaines", puis sélectionnez le domaine à configurer (exemple : stadium.local).

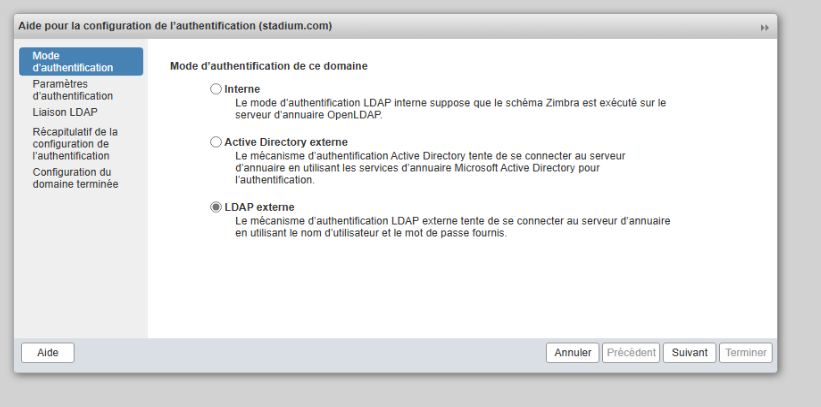
Dans la page de configuration du domaine, cliquez sur "Authentification".



**Étape 3 : Configuration des Paramètres LDAP**

Cliquez sur "Configurer la vérification des identifiants".

Choisissez "Utiliser une source d'authentification externe".



Renseignez les paramètres LDAP suivants :

Type d’authentification : LDAP

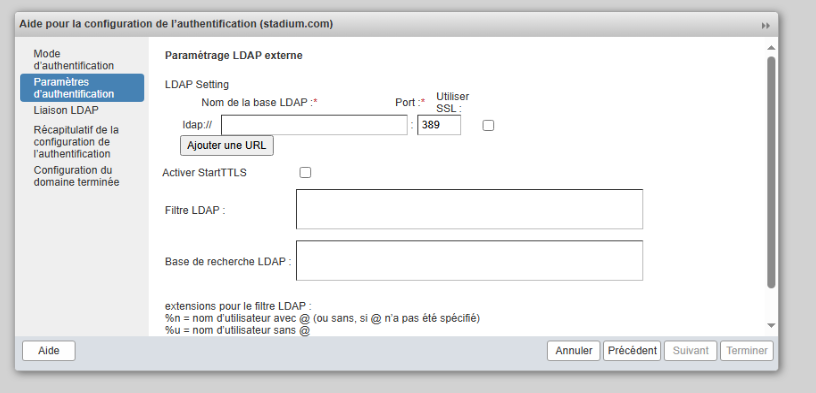
Serveur LDAP : 172.20.0.10

Port : 389 (ou 636 pour une connexion sécurisée via LDAPS)

BaseDN : DC=stadium,DC=local

Filtre de recherche : (sAMAccountName=%u) (Zimbra utilisera le nom d’utilisateur AD pour la connexion)

Mode de liaison LDAP : Anonyme ou Liaison simple avec un compte utilisateur (exemple : ldap\_bind@stadium.local et son mot de passe).



**Étape 4 : Test de la Connexion LDAP**

Cliquez sur "Test" pour vérifier la connexion entre Zimbra et Active Directory.

Si la connexion est réussie, cliquez sur "Enregistrer".

**Étape 5 : Test d’Authentification des Utilisateurs**

Accédez à l’URL client de Zimbra :  
https://172.20.0.13:8443/

Connectez-vous avec un compte utilisateur Active Directory (par exemple, prenom.nom@stadium.local).

Si la connexion réussit, cela confirme que l’authentification LDAP fonctionne correctement.