1. Configuration d'une authentification SAML pour Guacamole

Lien : https://guacamole.apache.org/doc/gug/saml-auth.html

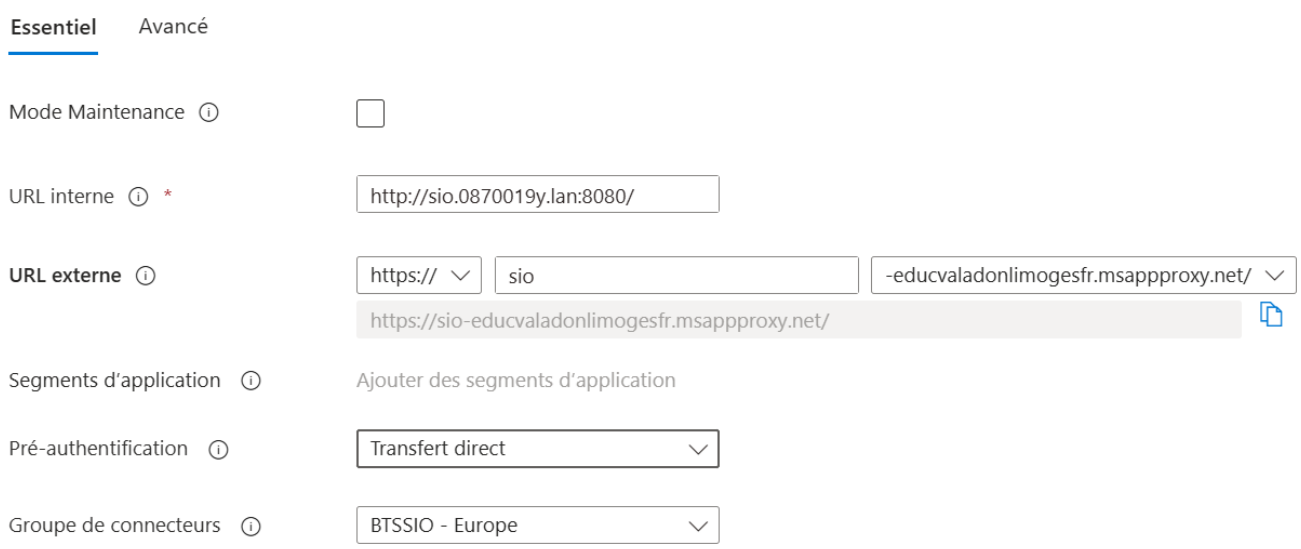
1.1. Installation de l'extension SAML pour guacamole

- Téléchargez guacamole-auth-sso-1.6.0.tar.gz, décompressez l'archive et déplacer guacamole-auth-sso-saml-1.6.0.jar dans le dossier extensions :

```
wget https://dlcdn.apache.org/guacamole/1.6.0/binary/guacamole-auth-sso-1.6.0.tar.gz
tar -xzf guacamole-auth-sso-1.6.0.tar.gz
sudo mv guacamole-auth-sso-1.6.0/saml/guacamole-auth-sso-saml-1.6.0.jar /etc/guacamole/extensions/
```

1.2. Publier l'application dans Azure

- Accéder au portail Azure → Microsoft Entra ID → Applications d'entreprise.
- Nouvelle application → Créer votre propre application.
- Choisir **Configurer le proxy d'application pour un accès à distance sécurisé à une application locale**



1.3. Configurer l'authentification SAML

- Accéder à l'application créee
- Dans l'application créée → Authentification unique → SAML.
- Renseigner :
  - Identificateur (Entity ID) : fourni par le service.
  - URL de réponse (ACS) : fourni par le service.
  - URL de connexion (facultatif) : page de login du service.

Télécharger le fichier de métadonnées XML d'Entra ID (il contient le certificat et les endpoints).

1.4. Configurer le service web avec les infos Entra ID

- Modifiez guacamole.properties avec les valeurs D'Entra ID :

```
sudo nano /etc/guacamole/guacamole.properties
```

Renseigner l'URI du fichier de métadonnées XML SAML d'Entra ID qui contient toutes les informations dont l'extension SAML de Guacamole a besoin pour savoir comment s'authentifier auprès de l'IdP Entra ID en renseignant le paramètre **saml-idp-metadata-url**. Dans Entra ID cette information est donnée à : **URL des métadonnées de fédération d'application**.

```
saml-idp-metadata-url: <App Federation Metadata Url>
```

L'URL que l'IdP utilisera une fois l'authentification réussie pour revenir à l'application web Guacamole et fournir les détails d'authentification à l'extension SAML. L'extension SAML ne prend actuellement en charge que le rappel en tant qu'opération POST vers cette URL de rappel. Cette propriété est obligatoire.

```
saml-callback-url: https://sio.0870019Y.lan:8080/ole.votre-domaine.com/api/ext/saml/callback
```

Pour le Débug

```
saml-debug: true
```

1.4.1. Contrôler le comportement de connexion

Guacamole charge les extensions d'authentification par ordre de priorité et évalue les tentatives d'authentification dans le même ordre. Cela a des implications sur le comportement du processus de connexion de Guacamole lorsqu'une extension SSO est présente :

- Si l'extension SSO a la priorité : Les utilisateurs qui ne sont pas encore authentifiés seront immédiatement redirigés vers le fournisseur d'identité configuré. Ils ne verront pas d'écran de connexion Guacamole.
- Si une extension non-SSO a la priorité : Les utilisateurs qui ne sont pas encore authentifiés verront un écran de connexion Guacamole. De plus, des liens vers le(s) fournisseur(s) d'identité configuré(s) seront disponibles pour les utilisateurs qui souhaitent se connecter via SSO.

La priorité par défaut des extensions est déterminée par leurs noms de fichiers, les extensions apparaissant plus tôt dans l'ordre alphabétique ayant une priorité plus élevée que les autres. Cela peut être modifié en définissant explicitement la priorité des extensions.

- Rediriger automatiquement tous les utilisateurs non authentifiés vers SAML, en donnant la priorité à l'extension SAML sur toutes les autres :

```
extension-priority : saml
```

- Présenter un écran de connexion Guacamole normal avec la possibilité de se connecter avec des identifiants traditionnels ou avec SAML, ne pas donner la priorité à l'extension SAML :

```
extension-priority : mysql, saml
```

- Redémarre Tomcat9

```
sudo systemctl restart tomcat9
```

- saml-entity-id: https://guacamole.votre-domaine.com/
- Fournir au service :
    - Entity ID d’Entra ID (souvent https://sts.windows.net/{tenant-id}/).
    - SSO URL : https://login.microsoftonline.com/{tenant-id}/saml2.
    - Certificat public (X.509) pour vérifier les signatures.

Importer le metadata XML d’Entra ID si le service le supporte.

 5. Attribuer des utilisateurs

Dans Entra ID → Utilisateurs et groupes → attribuer les comptes qui peuvent se connecter.

 6. Tester la connexion

Utiliser le bouton Tester l’authentification unique dans Azure. Vérifier les logs SAML (ACS du service) pour les assertions.

 Points clés

Format des claims : Par défaut, Entra ID envoie NameID (UPN). Vous pouvez personnaliser les attributs dans Attributs et revendications. Certificat : Surveillez la rotation automatique (Azure change le certificat tous les 3 ans). Sécurité : Activez la signature des assertions et la validation des audiences.

- Modification du fichier **guacamole.properties** pour configurer SAML.

```
sudo nano /etc/guacamole/guacamole.properties
```

- Ajoutez dans ce fichier les lignes suivantes :

```
# MySQL
```

```
mysql-hostname: 127.0.0.1
mysql-port: 3306
mysql-database: guacamole_db
mysql-username: guacamole_user
mysql-password: P@$$w0rd2025Secure
```

* Déclarez le serveur Guacamole (ici, on déclare une connexion locale sur le port par défaut, à savoir 4822).

```
sudo nano /etc/guacamole/guacd.conf
```

- Voici le code à intégrer :

```
[server]
bind_host = 0.0.0.0
bind_port = 4822
```

- Redémarrez les trois services liés à Apache Guacamole :

```
sudo systemctl restart tomcat9 guacd mariadb
```

From:
https://siocours.lycees.nouvelle-aquitaine.pro/ - **Les cours du BTS SIO**

Permanent link:
https://siocours.lycees.nouvelle-aquitaine.pro/doku.php/reseau/cloud/accesdistance/guacamoleauthsaml

Last update: **2026/01/12 14:34**