

Retour d'expérience GestSup - Entra ID sur hébergement IONOS

Résumé technique du problème rencontré avec GestSup 3.2.61 sur un hébergement mutualisé IONOS en PHP 8.4.24, ainsi que des contournements appliqués pour rétablir l'authentification et la synchronisation Entra ID.

Contexte

Élément	Valeur
GestSup	3.2.61
Hébergement en panne	IONOS mutualisé
PHP IONOS	8.4.24
Instance de comparaison	OVH
PHP OVH	8.0
Connecteur Entra ID	Même configuration sur les deux instances

Problème constaté

La configuration Entra ID était correcte : les mêmes Tenant ID, Client ID, secret et paramètres fonctionnaient sur l'instance OVH. En revanche, sur IONOS, les appels HTTP effectués par Guzzle/cURL vers **login.microsoftonline.com** renvoyaient un **HTTP 404**, avec un Content-Type **text/HTML** et un corps de réponse vide.

À l'inverse, les mêmes URL appelées depuis PHP avec **file_get_contents()** fonctionnaient correctement et retournaient le JSON attendu par Microsoft.

Exemple de symptôme initial

```
Fatal error: Uncaught TypeError: Cannot access offset of type string on string
vendor/thenetworg/oauth2-azure/src/Provider/Azure.php
```

La librairie attendait un tableau JSON contenant par exemple **authorization_endpoint**, mais recevait une chaîne de caractères ou une réponse non exploitable.

Tests réalisés

La découverte OpenID a été testée directement sur IONOS. Avec **file_get_contents()**, la réponse était valide : JSON correctement décodé, **authorization_endpoint**, **token_endpoint** et **issuer** présents.

Avec cURL, la même URL renvoyait : HTTP 404, Content-Type text/HTML, 0 octet de réponse. Le comportement restait identique en forçant HTTP/1.1.

Modifications appliquées

1. vendor/thenetworg/oauth2-azure/src/Provider/Azure.php

Trois appels HTTP ont été adaptés pour éviter le chemin Guzzle/cURL sur cet hébergement :

- Récupération de la configuration OpenID /.well-known/openid-configuration via `file_get_contents()` + `json_decode()`.
- Échange du code OAuth contre le token via un POST natif PHP avec `stream_context_create()` + `file_get_contents()`.
- Récupération des clés JWKS Microsoft via `file_get_contents()` + `json_decode()`.

Exemple de principe utilisé pour les requêtes POST :

```
$context = stream_context_create([
    'http' => [
        'method' => 'POST',
        'header' => "Content-Type: application/x-www-form-urlencoded\r\nAccept: application/json\r\n",
        'content' => $postData,
        'ignore_errors' => true,
    ]
]);
$response = file_get_contents($url, false, $context);
```

2. core/azure_ad.php

La synchronisation Entra ID utilisait explicitement Guzzle pour obtenir un token en `client_credentials`. Cet appel a été remplacé par un POST natif PHP, en conservant les mêmes paramètres : `client_id`, `client_secret`, `scope=https://graph.microsoft.com/.default` et `grant_type=client_credentials`.

3. connector.php

Le bouton « Test du connecteur Entra ID » avait son propre appel Guzzle vers `/oauth2/v2.0/token`. Le même remplacement a été appliqué pour que le test fonctionne lui aussi sur IONOS.

Résultat

Fonction	Résultat après correction
Connexion SSO Entra ID	OK
Échange OAuth / token utilisateur	OK
Validation JWT / JWKS	OK
Synchronisation Entra ID -> GestSup	OK
Bouton de test du connecteur Entra ID	OK

Conclusion pour le développeur

Le problème ne semble pas provenir de la configuration Entra ID. Il est reproductible sur l'hébergement IONOS lorsque GestSup passe par Guzzle/cURL vers `login.microsoftonline.com`. Sur le même serveur, le wrapper HTTP natif PHP fonctionne correctement. Un fallback vers `file_get_contents()/stream_context_create()`, ou une gestion plus robuste des réponses non JSON/HTTP 404, pourrait améliorer la compatibilité avec certains environnements mutualisés.