Mode Opératoire

Compte de service LDAP dédié pour Authentik (lecture seule)

Code :	MO-PLT-026
Version :	1.0
Date :	20 septembre 2026
Auteur :	Cédric LEGRAND
Classification :	USAGE INTERNE — Équipe BTS SIO

Historique des révisions

Version	Date	Modifications
1.0	20/09/2026	Création initiale — bind LDAP d'Authentik basculé sur le compte de service en lecture seule `svc-authentik-ldap`.

1 Objet

Ce mode opératoire décrit la création et l'usage du compte de service **`svc-authentik-ldap`**, qui porte le *bind* LDAP de la source « Active Directory BTS SIO » d'Authentik, ainsi que la procédure de bascule et de retour en arrière.

Jusqu'au 20/09/2026, Authentik lisait l'annuaire avec le compte **Administrateur du domaine** (`CN=Administrateur,CN=Users`) : un compte à pouvoir pour une simple lecture. Le compte de service dédié applique le principe de **moindre privilège** : en cas de fuite de son mot de passe (compromission d'Authentik, export de configuration), un attaquant ne peut que *lire* l'annuaire — droit que possède déjà tout utilisateur authentifié du domaine — au lieu de le modifier. C'est le même pattern que `svc-ldap-opnsense` (portail captif, MO-NET-008).

2 Champ d'application

Public concerné	Administrateurs de l'infrastructure BTS SIO (membres de `GG-AdminsPlateforme`)
Compte de service	`BTS\svc-authentik-ldap` (`CN=svc-authentik-ldap,OU=Serveurs,DC=bts,DC=sio`)
Consommateur	Source LDAP `ad-bts-sio` d'Authentik (`https://auth.docker.bts.sio`, CT 200)
Cible LDAP	DC1 — `ldaps://10.0.112.2`
Secret	Coffre Vaultwarden, item « AD — Compte de service svc-authentik-ldap »

3 Le compte de service

Le compte est créé dans l'OU `Serveurs` (même emplacement que `svc-ldap-opnsense`) avec les propriétés suivantes :

— **membre d'aucun groupe privilégié** — seul le groupe primaire « Utilisateurs du domaine », qui suffit à lire l'annuaire ;

— `PasswordNeverExpires` et `CannotChangePassword` (compte de service, rotation manuelle) ;

— mot de passe fort de 32 caractères, généré aléatoirement et versé au coffre à la création.

Commande de création (exécutée le 20/09/2026 via WinRM sur DC1) :

```
New-ADUser -Name 'svc-authentik-ldap' -SamAccountName 'svc-authentik-ldap' `
  -Path 'OU=Serveurs,DC=bts,DC=sio' -AccountPassword $sec -Enabled $true `
  -PasswordNeverExpires $true -CannotChangePassword $true `
  -Description 'Bind LDAP lecture seule pour Authentik (SSO plateforme Docker)'
```

4 Bascule du bind Authentik

1 Tester le bind avant toute bascule

Depuis un poste jointe au VLAN admin (ou le VPN collègues, qui autorise le 636), valider que le compte lit bien l'annuaire — par exemple en Python (`ldap3`) : bind LDAPS sur `10.0.112.2:636` avec `BTS\svc-authentik-ldap`, puis recherche `(memberOf=CN=GG-AdminsPlateforme,OU=Profs,DC=bts,DC=sio)` sous `DC=bts,DC=sio`. Attendu : les 6 comptes du groupe. Ne pas poursuivre si ce test échoue.

2 Pointer la source LDAP sur le compte de service

Dans l'interface d'administration Authentik : Directory → Federation and Social login → « Active Directory BTS SIO » → Edit.

Renseigner :

— ***Bind CN*** **:** `CN=svc-authentik-ldap,OU=Serveurs,DC=bts,DC=sio`

— ***Bind Password*** **: le mot de passe du coffre (bouton Modify) puis Update.**

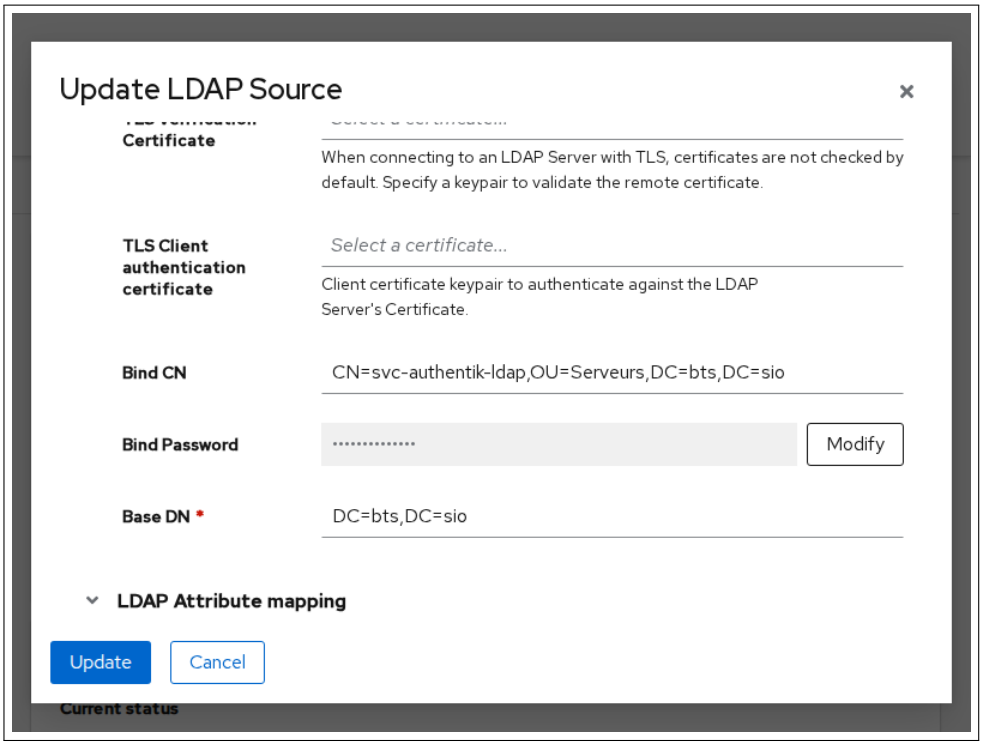

Figure 1 : La source LDAP après bascule : le bind n'utilise plus le compte Administrateur du domaine mais le compte de service en lecture seule.

Équivalent API (utilisé le 20/09/2026) : `PATCH /api/v3/sources/ldap/ad-bts-sio/` **avec** `bind_cn` **et** `bind_password` **— noter que l'adressage se fait par slug (l'adressage par pk renvoie 404 sur cette version).**

3 Forcer une synchronisation et vérifier

Sur la page de la source, bouton de synchronisation (ou `docker`

`exec authentik-server ak ldap_sync ad-bts-sio` **sur CT 200). Vérifier dans l'onglet Overview :** ***Last sync status : Successful*****, connectivité** `10.0.112.2: ok`**.**

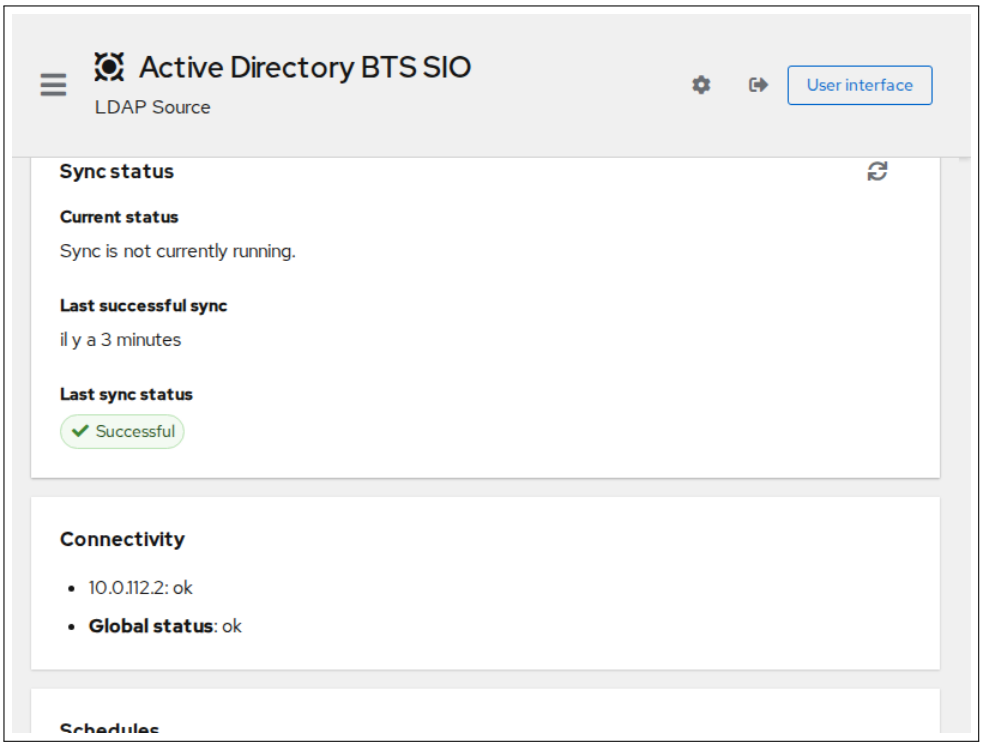

Figure 2 : Synchronisation réussie avec le compte de service : statut *Successful* et connectivité LDAPS vers DC1 confirmée.

Contrôler ensuite que les comptes et groupes AD sont toujours présents (Directory → Users / Groups) : les 6 administrateurs de `GG-AdminsPlateforme` **doivent figurer dans Authentik.**

4 Valider la chaîne complète

Ouvrir un service protégé (ex. `https://grafana.docker.bts.sio`**) dans une fenêtre de navigation privée et se connecter à la porte avec un compte AD du groupe : l'authentification AD passe par**

> **le bind de la source — ce test prouve la chaîne de bout en bout.**

5 Vérification

Vérification

- ☐ `Get-ADUser svc-authentik-ldap -Properties MemberOf` **sur DC1 : aucun groupe privilégié**
- ☐ **Bind LDAPS de test depuis le poste : 6 membres de** `GG-AdminsPlateforme` **retournés**
- ☐ **Source Authentik : *Bind CN* =** `CN=svc-authentik-ldap,...`**, sync *Successful***
- ☐ **Login AD réel à la porte sur un service OIDC (Grafana) après bascule : succès**
- ☐ **Mot de passe du compte de service présent en coffre**

6 Retour en arrière

Si la lecture LDAP venait à échouer après bascule (sync en erreur, logins AD refusés) : dans le même formulaire de la source, remettre *Bind CN* à `CN=Administrateur,CN=Users,DC=bts,DC=si` avec le mot de passe du coffre (item « DC1 — Srv2022 HyperV »), puis relancer une synchronisation. Le compte de service peut alors être désactivé (`Disable-ADAccount`) le temps du diagnostic. Le compte `Administrateur` n'a subi **aucune modification** pendant ce chantier ; le compte local `akadmin` d'Authentik (secours) n'est pas impacté.

7 Notes d'exploitation

— **Rotation du mot de passe** : changer le mot de passe AD (`Set-ADAccountPassword`), mettre à jour le coffre puis le *Bind Password* de la source, et forcer une synchronisation.
— **Ne pas supprimer** le compte sans avoir repointé la source : la synchronisation Authentik tomberait en erreur et les logins AD à la porte échoueraient.
— La lecture de l'annuaire par ce compte est visible dans les journaux de DC1 (événements 4624/4662 si l'audit est activé).