BTS Services informatiques aux organisations **SESSION 2026**

ANNEXE VII-1-A : Fiche descriptive de réalisation professionnelle (recto)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation : 1**
Nom, prénom : Rjiba Yanis	**N° candidat : 2541521597**
Épreuve ponctuelle ☒ **Contrôle en cours de formation** ☐	**Date :** ..... / ..... /.....

Organisation support de la réalisation professionnelle
Plateforme NYM-IT

Intitulé de la réalisation professionnelle
Mise en place du SSO avec Keycloak

Période de réalisation : 2025-2026 ..... **Lieu :** CFA Saint Félix La salle .....
Modalité : ☒ **Seul(e)** ☐ **En équipe**

Compétences travaillées
- ☒ Concevoir une solution d'infrastructure réseau
- ☒ Installer, tester et déployer une solution d'infrastructure réseau
- ☒ Exploiter, dépanner et superviser une solution d'infrastructure réseau

Conditions de réalisation[1] (ressources fournies, résultats attendus)

Ressources fournies :
- Serveur Debian 13 (SRV-NYMIT) hébergeant Docker et les services conteneurisés
- Contrôleur de domaine Active Directory Windows Server (192.168.1.1), domaine NYM-IT.local
- Réseau local Vlan 1 :192.168.1.0/24 et réseau Docker sur Vlan 20 : 192.168.20.0/24
- Services existants à intégrer au SSO : Nextcloud 32 (VM 192.168.1.205) et GLPI 11 (conteneur Docker : 192.168.20.5 :10101)
- Accès administrateur au domaine AD et aux services existants

Résultats attendus :
- Solution SSO fonctionnelle permettant l'authentification unique sur Nextcloud, GLPI et un portail d'accès
- Fédération de l'Active Directory existant sans duplication ni migration de comptes
- Portail d'accès unifié offrant un point d'entrée unique aux utilisateurs
- Documentation technique détaillée et procédures de supervision et maintenance

[1] En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

Description des ressources documentaires, matérielles et logicielles utilisées[2]

Ressources matérielles :
- Serveur Proxmox hébergeant les machines virtuelles (SRV-NYMIT, DC, Nextcloud)
- Réseau commuté avec VLANs (LAN 192.168.1.0/24, Docker 192.168.20.0/24)

Ressources logicielles :
- Keycloak 26.5.2 (conteneur Docker, image quay.io/keycloak/keycloak)
- PostgreSQL 17 (conteneur Docker, base de données Keycloak)
- GLPI 11 + plugin samlSSO 1.2.5 (conteneur Docker) avec MariaDB 12
- Nextcloud 32 + plugin user_saml (VM dédiée Debian 13)
- Nginx (reverse proxy HTTPS, installé sur l'hôte Debian)
- Docker Engine + Docker Compose
- Portainer CE (gestion et supervision des conteneurs)
- Certificats auto-signés générés avec openssl

Ressources documentaires :
- Documentation officielle Keycloak (keycloak.org/documentation)
- Documentation Nextcloud SSO & SAML (docs.nextcloud.com)
- Documentation plugin samlSSO GLPI (github.com/derricksmith/phpsaml)
- Spécifications SAML 2.0 (OASIS) et OpenID Connect

[2] Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

Modalités d'accès aux productions[3] et à leur documentation[4]

Accès à l'environnement technique :
- Keycloak (IdP): https://keycloak.nym-it.local:8449/admin
- Portail SSO : https://portal.nym-it.local
- Nextcloud: https://nextcloud.nym-it.local
- GLPI: https://glpi.nym-it.local
- Portainer : https://portainer.nym-it.local:9443

Identifiants disponibles sur https://vaultwarden.nym-it.fr
Avec les identifiants suivants : admin@nym-it.fr et le mot de passe JaimeLeSwag44

Documentation :
- Documentation technique complète (PDF, jointe au dossier)
- Documentation de la structure Nym-it sur mon portfolio onglet épreuve: https://sio.campus-sfls.fr/PROMO%202426/RJIBA/epreuves.html

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

ANNEXE VII-1-A : Fiche descriptive de réalisation professionnelle (verso, éventuellement pages suivantes)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

[3] Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

[4] Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

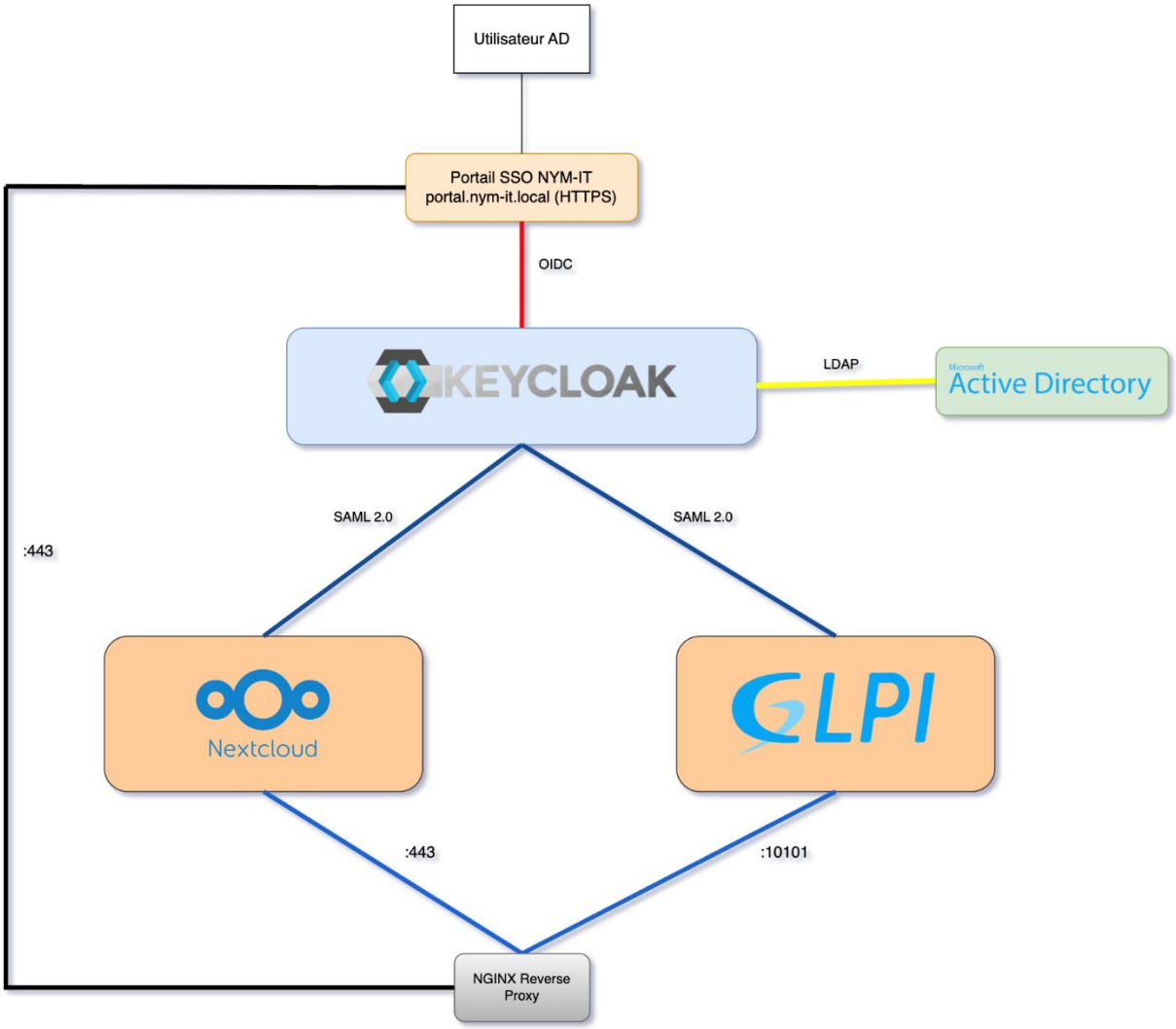
Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs

Cette réalisation porte sur le déploiement d'une solution d'authentification centralisée (SSO) avec Keycloak au sein de l'infrastructure NYM-IT. L'objectif est de remplacer les connexions LDAP individuelles de chaque application par un Identity Provider unique, fédérant l'Active Directory existant et offrant un accès SSO via les protocoles SAML 2.0 et OIDC.

1. Analyse de l'existant et conception de l'architecture

L'infrastructure existante comprenait plusieurs services (Nextcloud, GLPI, Portainer, UrBackup) authentifiant chacun les utilisateurs via des connexions LDAP directes vers l'Active Directory. Cette approche posait des problèmes de redondance de configuration, d'absence de session partagée et d'impossibilité d'ajouter des utilisateurs externes.

L'architecture conçue place Keycloak comme point central d'authentification. Keycloak est accessible en HTTPS sur le port 8449 (sans passer par le reverse proxy Nginx, pour éviter les problèmes de headers de proxy avec SAML). Nginx assure le reverse proxy HTTPS pour GLPI, Nextcloud et le portail.



2. Déploiement de Keycloak via Docker Compose

Keycloak 26.5.2 a été déployé en conteneur Docker avec PostgreSQL 17 comme base de données. La configuration repose sur des variables d'environnement (KC_HOSTNAME, KC_HOSTNAME_STRICT, certificats SSL montés en volume). Un healthcheck pg_isready assure que PostgreSQL est prêt avant le démarrage de Keycloak.

3. Fédération LDAP avec Active Directory

La fédération LDAP a été configurée en mode READ_ONLY avec un compte de service dédié (Sync_keycloack) disposant de droits de lecture seule. L'attribut sAMAccountName a été choisi comme identifiant (plutôt que UserPrincipalName) pour obtenir des noms courts. 14 utilisateurs ont été synchronisés depuis l'OU SERVICES de l'AD NYM-IT.local.

4. Intégration SAML 2.0 avec Nextcloud

Un client SAML a été créé dans Keycloak pour Nextcloud (Entity ID : https://nextcloud.nym-it.local). Le plugin user_saml de Nextcloud a été configuré avec le mappage des attributs (username, email, groups avec préfixe saml_). L'option multi-authentification a été activée pour conserver un accès admin local de secours.

5. Intégration SAML 2.0 avec GLPI

L'intégration GLPI a été la partie la plus complexe du projet. Le plugin samlSSO 1.2.5 a été installé manuellement dans le conteneur Docker (/var/glpi/marketplace/). Plusieurs spécificités non documentées ont été découvertes et résolues : trailing slash obligatoire dans le Client ID, activation de COMPRESS REQUESTS, suppression des scopes SAML par défaut (role_list, saml_organization), Name ID format email avec Force ON, Force POST binding OFF.

6. Portail d'accès unifié (OIDC)

Un portail web (HTML/CSS/JS) a été développé, utilisant le protocole OIDC (Authorization Code Flow) pour authentifier l'utilisateur auprès de Keycloak. Le portail propose des liens IdP-initiated SAML vers Nextcloud et GLPI. Il est servi en HTTPS par Nginx.

7. Supervision et maintenance

La supervision comprend : monitoring des conteneurs via Portainer (statistiques CPU/RAM, logs en temps réel), script Bash de Heath check automatique avec redémarrage du conteneur toutes les 5 minutes, et cron de nettoyage des loginstates GLPI (purge toutes les minutes pour éviter les erreurs de race condition).

8. Incidents résolus

19 incidents techniques ont été rencontrés et documentés au cours du projet :
- KC-01 à KC-04 : port d'accès, hostname strict, URL metadata, JGroups
- LDAP-01/02 : format username (UPN vs sAMAccountName), persistance des anciens usernames
- NC-01 à NC-04 : Entity ID mismatch, certificat corrompu, NameID format, compte non approvisionner
- GLPI-01 à GLPI-08 : chemin plugin Docker, attributs doublons, loginstate corrompu, compression SAML, trailing slash, healthcheck MariaDB
- PORTAL-01/02 : URLs IdP-initiated encodées, redirect URI invalide

Chaque incident est documenté avec son symptôme, sa cause racine, sa résolution et sa prévention dans la documentation technique complète.