Konfigurierbare LDAP-Anbindung

Anbei ein paar Informationen für Schuladministratoren und Techniker, die Nutzerauthentifizierung der NBC über ein individuelles LDAP nutzen wollen.

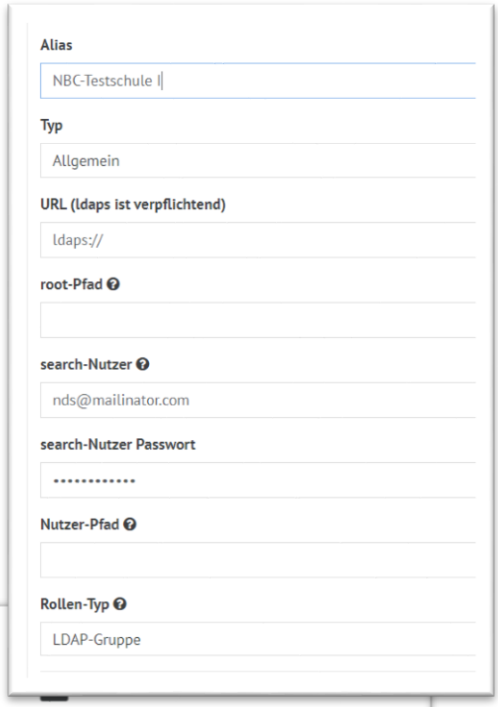
Die Dokumentation des HPI dazu befindet sich hier: https://docs.schul-cloud.org/pages/viewpage.action?pageId=55902270

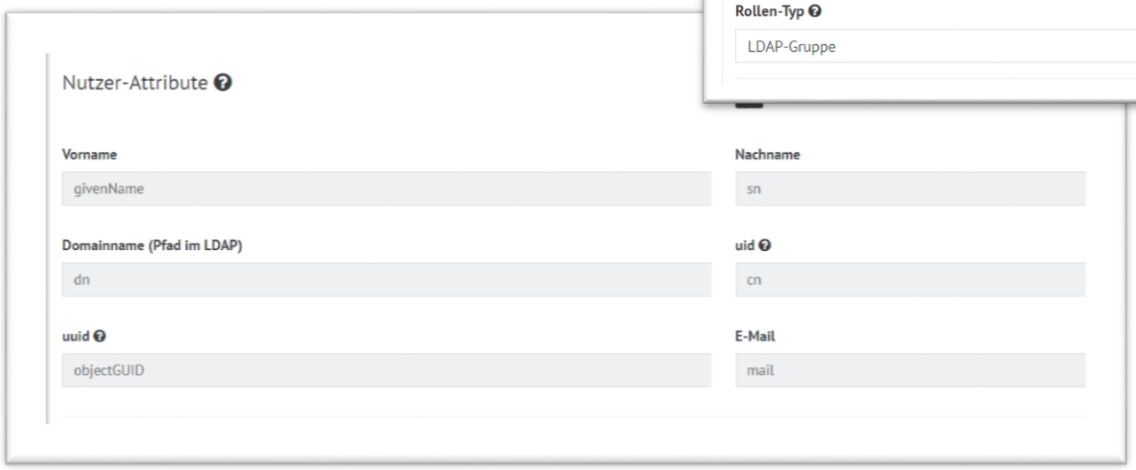
Vorbereitung

- Der LDAP der Schule muss von außen über eine LDAPS-Verbindung erreichbar sein. GGf. müssen in einer Firewall folgende IP-Adressen freigegeben werden: 141.89.221.180 (HPI) und 78.46.103.254 (NBC).
- Der LDAP muss sich mit einem Zertifikat ausweisen, dass von einer der anerkannten CA ausgestellt wurde. Let's Encrypt-Zertifikate funktionieren auch.
- Es muss ein Search-User zum Auslesen und Synchronisieren des Verzeichnisses angelegt werden, der möglichst nur Leserechte haben sollte.

Für die Konfiguration erforderliche Angaben zum LDAP-Verzeichnis

- Root-Pfad und Pfad(e) zu den Nutzern
- Die in der Eingabemaske benannten Nutzer-Attribute müssen bekannt und vorhanden sein. Attributsnamen sind wählbar
- Die E-Mail muss für jeden User systemweit über die gesamte NBC einmalig sein, ebenso die UUID.



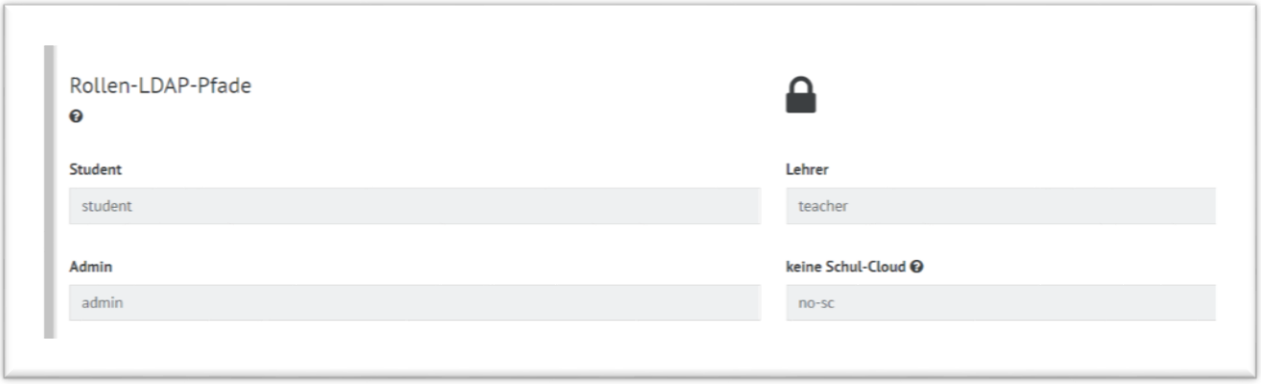


Es werden nur Nutzer mit Rollen synchronisiert. Die Rollenzuweisung ist (a) entweder durch eine Gruppenzugehörigkeit mit „memberOf“-Attribut oder (b) alternativ über eine frei definiertes Attribut, dass die Rolle direkt beschreibt, möglich. Die Auswahl geschieht über „Rollen-Typ“.

Fall (a), Rollenzuweisung durch Gruppenzugehörigkeit

Bei Rollen-Typ „LDAP-Gruppe“ auswählen und die LDAP-Gruppen für Schüler, Lehrer und Admin als vollen Pfad inkl. Root-DN angeben.

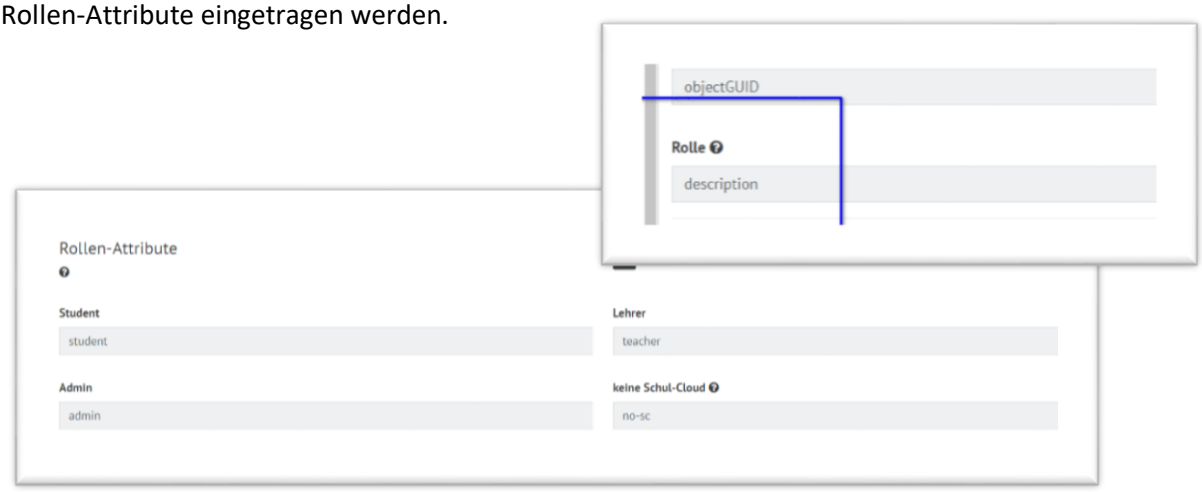
Die Gruppen-/Rollenzugehörigkeit der User muss durch das User-Attribut „memberOf“ gegeben sein.



Fall (b), Rollenzuweisung durch ein Attribut

Bei Rollen-Typ „Nutzer-Attribut“ auswählen und bei „Rolle“ den Namen des Attributs eingeben.

Die Werte des Attributs für die jeweiligen Rollentypen (Schüler, Lehrer, Admin) müssen dann bei Rollen-Attribute eingetragen werden.



Klassenzuweisung

Für Klassen- und Gruppenzuweisungen kann optional ein Pfad zu den Klassen-Gruppen angegeben werden. Alle Gruppen unter diesem Pfad werden als Klassen in der NBC abgebildet.