Handbuch:Erweiterung/LDAP Authentication

Eine freigegebene Version dieser Seite, freigegeben am *30. Juli 2020*, basiert auf dieser Version.

LDAP bedeutet Lightweight Directory Access Protocol (leichtgewichtiges Verzeichnisprotokoll). Dies kann zur zentralen Authentifzierung genutzt werden. Diese Erweiterung ermöglicht die Anbindung von BlueSpice (und MediaWiki) an einen LDAP-Server zur zentralen Authentifizierung.

Wichtig! Aufgrund einer Sicherheitslücke bei Active Directory wird dringend die Verwendung einer gesicherten Verbindung (mit SSL/TLS-Verschlüsselung) zur Benutzerauthentifizierung empfohlen. Microsoft veröffentlicht im März 2020 einen Patch, der keine ungesicherten Verbindungen mehr zulässt:

https://portal.msrc.microsoft.com/de-de/security-guidance/advisory/ADV190023
https://support.microsoft.com/de-de/help/4520412/2020-ldap-channel-binding-and-ldap-signing-requirement-for-windows

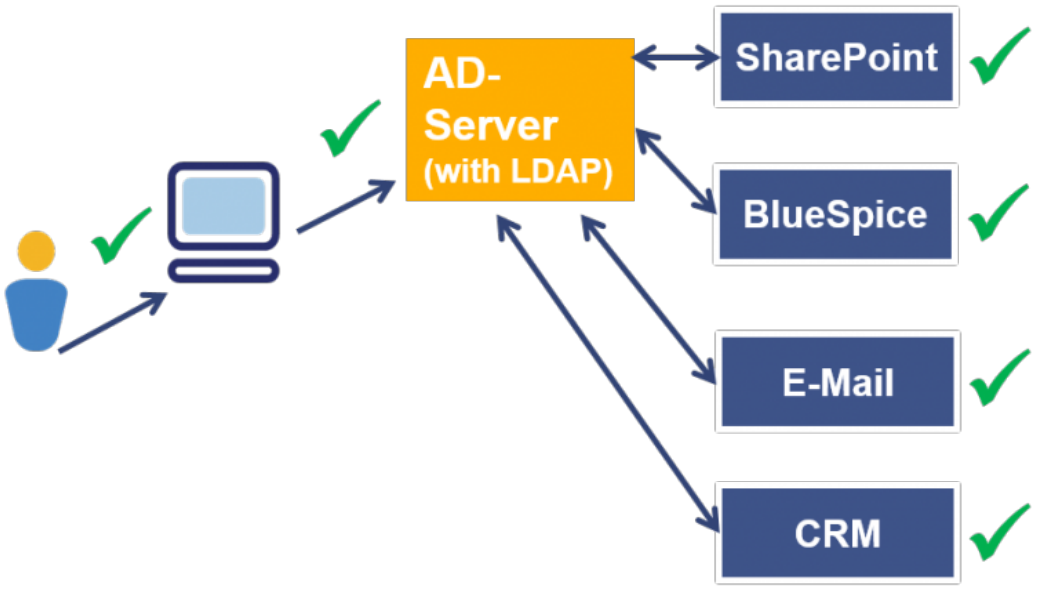
Betroffen ist jede Software, die LDAP-Abfragen über nicht gesicherte Verbindungen herstellt. Dies betrifft je nach Einstellungen ggf. auch BlueSpice MediaWiki. Sofern Ihr System so konfiguriert ist, dass es bereits eine gesicherte Verbindung verwendet, ist nichts zu tun.

Sollten BlueSpice und Active Directory über eine nicht gesicherte Verbindung kommunizieren, muss das System nachkonfiguriert werden, um erreichbar zu bleiben. Bitte prüfen Sie Ihre Konfigurationen und kontaktieren Sie uns bei Fragen zu diesem Thema.

Inhaltsverzeichnis

BlueSpice mit LDAP

Die MediaWiki-Erweiterung "LDAP Authentication" ist standardmäßig in BlueSpice free vorhanden, jedoch **nicht standardmäßig aktiviert**. Um das Wiki an LDAP anzubinden ist eine Aktivierung der Extension und deren Konfiguration notwendig.



Konfigurationsmöglichkeiten

LDAP	Anbindung an ein AD ohne Gruppensynchronisierung
LDAP mit Gruppensynchronisierung	Haben Sie für Ihr Unternehmen bereits definierte Benutzergruppen angelegt, können diese für das Wiki übernommen werden. Die entsprechenden Gruppen sind dann mit dem Gruppennamen automatisch im Wiki vorhanden und Sie können dort noch den Gruppen die entsprechenden Wiki-Rechte zuweisen.
Comfort Sign-on	wie LDAP mit Gruppensynchronisierung Um die Anbindung an eine zentrale Authentifizierung zusätzlich weiter auszubauen, gibt es die Möglichkeit ein Single Sign-On einzurichten. Damit ist der Benutzer direkt bei der Anmeldung am PC auch gleichzeitig am Wiki angemeldet.

Nach der Konfiguration von LDAP zu beachten:

- Das Wiki schreibt nicht in das LDAP-Verzeichnis zurück.
  Das bedeutet, dass z.B. Passwortänderungen im Wiki zum Konflikt führen können, im besten Fall aber beim nächsten Login von LDAP überschrieben werden.
- User dürfen niemals im Wiki händisch angelegt werden, dies führt zum Konflikt, selbst wenn man die Konvention der Groß- und Kleinschreibung der LdapAuthentication befolgt.
- Über die Benutzerverwaltung lassen sich keine Benutzer im LDAP-Verzeichnis anlegen.
- Standardmäßig findet keine initiale und/oder aktive Synchronisierung mit dem LDAP-Verzeichnis statt. User tauchen erst nach dem erstmaligen Login im Wiki auf.
- Eine Gruppenzuweisung ist über das Wiki möglich.

für die LDAP Konfiguration mit Gruppensynchronisierung gilt zudem:

- Auch hier ist das AD die führende Instanz, d.h. Gruppen werden aus dem AD übernommen.
  Vorsicht: Die entsprechende Gruppe muss mit dem identischen Namen, wie sie im AD-Verzeichnis heißt, im Gruppenmanager des Wikis angelegt werden, um die Gruppenzuweisung zu garantieren.
- Gruppen dürfen im Wiki nicht händisch dem User zugewiesen werden. Nehmen Sie bitte die Zuweisung über das LDAP-Verzeichnis vor.
- Gruppen, denen ein User im LDAP-Verzeichnis nicht angehört, werden ihm im Wiki nicht angezeigt.
- Die Zuweisung des Users zu Gruppen findet während der Login-Routine beim jeweiligen User statt, auch hier gilt: kein automatischer Abgleich mit dem Verzeichnis im Hintergrund.
- Eine Gruppenzuweisung über das Wiki ist nicht möglich. Ausnahmen sind die Gruppen sysop, bot und bureaucrat. Diese können über das Wiki zugewiesen werden und werden auch nicht dem User entzogen.

für die LDAP Konfiguration mit Comfort Sign-on gilt zudem:

- Browservoraussetzungen: kompatibel mit Internet Explorer, Edge und Google Chrome.
- Voraussetzung: Aufruf des Wikis über https, nicht http.
- Die Webseite muss entsprechend dem lokalen Intranet zugewiesen sein (Gruppenrichtlinie)

Weblinks

Dokumentation auf Mediawiki.org