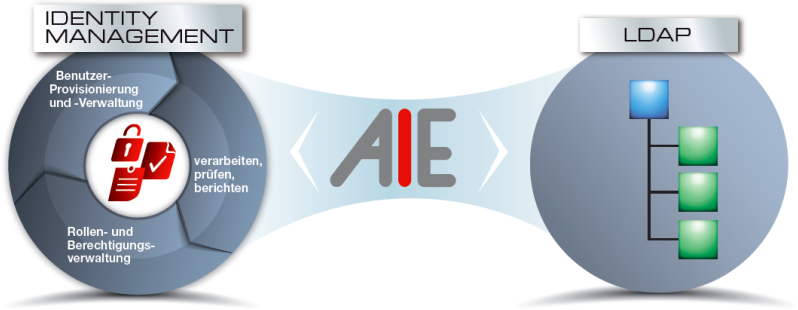
Identity und Access Management in LDAP Umgebungen



Das Lightweight Directory Access Protocoll – kurz LDAP – steht heute als De Facto Standard für die Authentifizierung und Autorisierung von Anwendern an einer Vielzahl von Unternehmensanwendungen. Folglich sind heute eine ganze Reihe von LDAP Verzeichnisserver-Produkten verfügbar, welche teilweise als Einzellösungen, teilweise aber auch in multiplen Instanzen für mehrere Unternehmensanwendungen eingesetzt werden. Die Herausforderungen sind hier Qualitätssicherung bei der Verwaltung der Benutzerdaten sowie einheitliche Provisionierungs- und De- Provisionierungsprozesse.

Advanced Integration Elements für LDAP

Das Advanced Integration Element für LDAP (AIE-LDAP-Root) ist das technische Bindeglied zwischen dem Identity and Access Management System (IAMS) und dem LDAP Verzeichnisserver als Zielsystem. Es wickelt die Provisionierungs- und De-Provisionierungsprozesse für digitale Identitäten, LDAP Benutzerkonten, Gruppen sowie die technischen Berechtigungsprozesse im Hintergrund ab.

Die Implementierung eines AIE-LDAP-Root beinhaltet[1]:

- Synchronisation der Benutzerkonten- und Gruppeninformationen – uni- oder bidirektional
  - Anlegen von Benutzerkonten- und Gruppenobjekten
  - Modifizieren von Benutzerkonten- und Gruppenobjektinformationen
  - Löschen von Benutzerkonten- und Gruppenobjekten
  - Aktivieren oder Sperren von Benutzerkonten[2]
- Umsetzung einer Bildungsregel für Benutzerkontennamen im LDAP Verzeichnis
- Synchronisation des Standard Informations-/Datensatzes (Attribute)[3] eines Objektes
- 1:1 Synchronisation der Attributwerte (keine Modifikation)
- Synchronisation des Passwortes für den LDAP Benutzer
- Synchronisation der Objekte in einen einzelnen Container des LDAP-Verzeichnisses (flach) oder Spiegeln und Synchronisieren hierarchischer Strukturen oder
- Platzierung der Objekte auf Basis bestimmter Attributwerte – z. B. Abteilung oder Lokation
- Implementierung des AIE-LDAP-Root im vorhandenen IS4IT AIE-IAM-System (single stage)[5]
- Basis-Systemdokumentation in Form eines technischen Anbindungsdatenblattes

Optional können die AIE wie folgt angepasst und erweitert werden:

- AIE zur Übernahme von Personenstammdaten aus vorhandenen Personalführungssystemen
- AIE zur Überprüfung des Passwort-Synchronisationsstatus über das IAMS
- Zuweisung von Standard-Berechtigungsprofilen auf Basis automatischer LDAP Gruppenmitgliedschaften bei der Benutzerkonten-Provisionierung

- Durchführen von Attribut-Transformationen – z. B. Füllen des Beschreibungsfeldes („description“ Attribut) eines LDAP Benutzerkontos nach Kundenvorgabe
- AIE für erweitertes Reporting und Historisierung zur Erfüllung gesetzlicher Anforderungen hinsichtlich der Aufbewahrungsfrist
- Erweiterung um zusätzliche Anbindungsserver (RemoteLoader) zur Erhöhung der Ausfallsicherheit einer LDAP Anbindung an das IAMS
- Erweiterung um weitere LDAP Verzeichnisse
- Erweiterung um zusätzliche Stages, z. B. für Entwicklungs-, Test- und Produktionsumgebung – Rabattierung möglich!

Mit dem optional erhältlichen elektronischen Antragswesen für digitale Identitäten, Zielsystem-Benutzerkonten und Berechtigungen auf Basis der **IS4IT Advanced Form Elements (AFE)** können Genehmigerstellen in den Antragsprozess eingebunden werden. Die Umsetzung genehmigter Anträge erfolgt je nach Anbindungsart des Zielsystems vollautomatisch oder administrativ über entsprechende Benachrichtigungen der Systemverwalter.

Mit den ebenfalls optional erhältlichen **IS4IT Advanced Documentation Objects (ADO)** wird eine erweiterte, umfängliche Dokumentation bereitgestellt, die neben der kundenspezifischen Architekturbeschreibung eine vollständige Prozessdokumentation beinhaltet.

Wartung und Support des AIE, d. h. die Versorgung der Software mit Aktualisierungen bzw. Patches, sind während der Implementierungsphase bis zur Inbetriebnahme ebenso enthalten wie die Unterstützung bei der Entstörung im Fehlerfall. Der Bezug von Weiterentwicklungen und AIE Updates ist anschließend im Rahmen gesonderter Abkommen möglich.

Hinweise und Einschränkungen:
[1] Alle nicht genannten Funktionen sind nicht enthalten oder als Option verfügbar
[2] Sofern vom LDAP Verzeichnisserver unterstützt
[3] Werden bei der Anforderungsdefinition (Lastenheft) bzw. vor der Implementierung abgeglichen
[4] Kostenpflichtig, Voraussetzung für Implementierung der AIE-AD-Root