Identity und Access Management in Microsoft Windows Umgebungen

Advanced Integration Elements für Active Directory

Das Advanced Integration Element für Active Directory (AIE-AD-Root) ist das technische Bindeglied zwischen dem Identity Management System (IDMS) und dem Zielsystem Microsoft Active Directory. Es wickelt die Provisionierungs- und De-Provisionierungsprozesse für digitale Identitäten, AD Benutzerkonten sowie die technischen Berechtigungsprozesse im Hintergrund ab.

Die Implementierung eines AIE-AD-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
- Umsetzung einer Bildungsregel für Benutzerkontennamen im Active Directory
- Zuweisung von Standard-Berechtigungsprofilen auf Basis automatischer AD Gruppenmitgliedschaften bei der Benutzerkonten-Provisionierung
- Synchronisation des Standard Informations-/Datensatzes (Attribute)[2] eines Objektes
- 1:1 Synchronisation der Attributwerte ohne Modifikation
- Synchronisation der Passwörter[3]
- Synchronisation der Objekte in einen einzelnen Container des AD (flach) oder Spiegeln und Synchronisieren hierarchischer Strukturen oder
- Platzierung der Objekte auf Basis bestimmter Attributwerte – z. B. Abteilung oder Lokation
- Implementierung des AIE-AD-Root im vorhandenen IS4IT AIE-IAM-System (single stage)[4]
- 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 IDMS
- AIE zur Ausführung von benutzerdefinierten Powershell Kommandos und Scripten im Rahmen eines erweiterten Identity & Access Managements in AD Umfeldern
- AIE zur vollständigen Anbindung von Microsoft Exchange (Provisionierung und De-Provisionierung)
- Durchführen von Attribut-Transformationen – z. B. Füllen des Beschreibungsfeldes („description“ Attribut) eines AD Benutzerkontos nach Kundenvorgabe
- AIE für erweitertes Reporting und Historisierung zur Erfüllung gesetzlicher Anforderungen hinsichtlich der Aufbewahrungsfrist
- AIE zur Ausführung weiterer Aktionen im Active Directory bzw. auf den Windows Servern – z. B. Ausführen von Powershell oder anderen Kommandos und Scripten, Operationen im Dateisystem usw.

- AIE zur dauerhaften Speicherung der SID des AD Benutzerkontos im IDMS – Vereinfachung von AD Migrationen unter Beibehaltung von Berechtigungen (ACL)
- Erweiterung um zusätzliche Anbindungsserver (RemoteLoader) zur Erhöhung der Ausfallsicherheit einer AD Anbindung an das IDMS
- Erweiterung um weitere Active Directory Domänen – Kostenersparnis über Rabattierung möglich!
- 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 im 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] Werden bei der Anforderungsdefinition (Lastenheft) bzw. vor der Implementierung abgeglichen
[3] Für die Passwort-Synchronisation ist die Installation eines Passwort-Filterservices auf allen vollwertigen Domain Controllern erforderlich (keine Read-only DCs)
[4] Kostenpflichtig, Voraussetzung für Implementierung der AIE-AD-Root