

Setup Voraussetzungen

Handbuch für Administratoren

Access Manager Password Reset 2023.2

Hinweise zur Installations-Vorbereitung

BAYOOSOFT
MANAGEMENT SOFTWARE

Inhalt

1 GLOSSAR 2

2 VORBEREITENDE AUFGABEN 3

2.1 Checkliste – Schnellübersicht 3

2.2 AMPR Server 4
2.2.1 Hardware AMPR Server 4
2.2.2 Software AMPR Server 4
2.2.3 Hardware DB Server 4
2.2.4 Software DB Server 5

2.3 DNS-Eintrag 5

2.4 Benutzerkonten 5

2.5 SMTP-Gateway 7

2.6 Firewall & offene Ports 7
2.6.1 Webserver 7
2.6.2 Active Directory / LDAP 7
2.6.3 Datenbank 7

2.7 Datenbank 7

1 Glossar

Begriff	Bedeutung
AMPR	BAYOOSOFT Access Manager Password Reset
AD	Active Directory
SSL	Secure Socket Layer
MS SQL Server	Microsoft SQL Datenbank Server

2 Vorbereitende Aufgaben

Dieses Dokument beschreibt die notwendigen infrastrukturellen Voraussetzungen, die für eine erfolgreiche Installation des Access Manager Password Reset (AMPR) in Ihrer Umgebung vorab erfüllt sein müssen.

2.1 Checkliste – Schnellübersicht

Die folgenden Vorbereitungen müssen durchgeführt werden. Haken Sie ab, was bereits erledigt ist. Detaillierte Informationen zur Durchführung finden Sie jeweils in den folgenden Kapiteln.

Erledigt	Aufgabe
☐	Hardware-Anforderungen erfüllen
☐	Software-Anforderungen erfüllen
☐	DNS-Einträge anlegen (optional, aber empfohlen)
☐	(AMPR-)Benutzerkonten anlegen
☐	Zugang zum Email-Server sicherstellen
☐	Firewall & Ports öffnen
☐	Datenbank anlegen & AMPR-Benutzerkonten berechtigen

2.2 AMPR Server

Die Hardware-Anforderungen orientieren sich an einer Installation für Testzwecke mit überschaubarer Last, allerdings schon mit Blick auf eine spätere Weiternutzung als Produktivsystem, was viele Kunden bevorzugen. Da das Leistungsprofil in jedem Unternehmen unterschiedlich ist, können hier keine konkreten Aussagen über die Anforderungen an einen Produktivserver gemacht werden. Wenden Sie sich hierzu bitte an unseren Support.

Es werden zwei (virtuelle) Server benötigt, einer der die AMPR Websites und den AMPR-Server (als Windows-Dienst) hostet und einer, der den MS SQL Server sowie die von ihm verwaltete Datenbank für AMPR hostet. Alle Hardware-Angaben sind empfohlene Mindestanforderungen.

2.2.1 Hardware AMPR Server

Komponente
12 GB RAM
2 CPU mit 2 GHz Takt
20 GB Festplattenspeicher

2.2.2 Software AMPR Server

Komponente	Anmerkung
Windows Server 2016 Windows Server 2019	Auf dem Server müssen alle aktuellen Patches installiert sein.
Microsoft Visual Studio 2010 (VC++ 10.0) SP1 (64 Bit)	https://www.microsoft.com/de-DE/download/details.aspx?id=26999
Microsoft Visual C++ Redistributable-Pakete für Visual Studio 2015, 2017, 2019 und 2022 (64 Bit)	https://aka.ms/vs/17/release/vc_redist.x64.exe
sapjco3.dll und sapjco3.jar	Diese Dateien werden nur benötigt, wenn eine Anbindung an SAP erfolgen soll. Die Dateien können ausschließlich durch den Kunden über das SAP-Portal bezogen werden.

2.2.3 Hardware DB Server

Komponente
12 GB RAM
2 CPU mit 2 GHz Takt
50 GB Festplattenspeicher

2.2.4 Software DB Server

Komponente	Anmerkung
Windows Server 2016 Windows Server 2019	Auf dem Server müssen alle aktuellen Patches installiert sein.
MS SQL Server Express 2016 bis 2019 MS SQL Server 2016 bis 2019	

2.3 DNS-Eintrag

Es wird empfohlen, dass die AMPR Webseiten unter einem Namen erreichbar sind, der von dem Server-(DNS-)Namen unabhängig ist. Dies bietet Ihnen die Freiheit, den AMPR-Server (später) auf eine andere Maschine umzuziehen und außerdem dem AMPR-Anwender eine URL zur Verfügung zu stellen, die den Anwendungszweck bereits über den Namen vermittelt (z.B.: Passwort-SelfService.ihre-domain.local).

Hierzu ist ein eigener DNS-Eintrag einzurichten, der auf den AMPR-Server zeigt. Im Regelfall reicht ein einziger DNS-Eintrag aus, also bspw.:
http://passwort-selfservice.ihre-domain.local

Bitte verwenden Sie keine Unterstriche („_“) in den DNS-Namen, dies führt bei Nutzung von Java und des Internet Explorers zu Fehlfunktionen.

Es wird empfohlen, Alias-Einträge (CNAME) einzurichten.

2.4 Benutzerkonten

AMPR benötigt Benutzerkonten:

- Falls der AMPR-Server-Dienst unter einer eigenen Kennung laufen soll.
- Eine Kennung über die sich AMPR an das DBMS anmelden kann.
- Je eine Kennung, mit der AMPR auf dem jeweiligen Zielsystem (Windows-AD, LDAP-System, SAP-System) einen PW-Reset durchführen soll.
- Ein Email-Account, falls AMPR Emails versenden soll, für die eine Authentifizierung erforderlich ist (SMTPAuth).

Die Kennungen (bzw. Kennungsnamen) können disjunkt sein, müssen es aber nicht.

Die Kennungen müssen über die nachfolgenden Rechte verfügen. Diese müssen ggf. explizit gewährt werden. Beachten Sie, dass eventuelle globale Gruppenrichtlinien lokal gesetzte Richtlinien überschreiben und damit eine lokale Rechtevergabe aufheben könnten.

Berechtigungen für den Windowsdienst:

- Log on as a service (Anmelden als Dienst)
- Kein Ablaufdatum des Passworts

Berechtigungen für den Windows AD Zugriff:

- Lesenden Zugriff auf die Benutzerdaten (in den OUs, die durch AMPR unterstützt werden sollen). Sollen bestimmte Benutzerkonten durch AMPR nicht berücksichtigt werden (z.B. von ausgeschiedenen Personen oder archivierten Accounts), so sollte dem AMPR AD-Account für die betreffenden OUs das Leserecht per Deny entzogen werden.
- Accountsperren (wegen zu vieler fehlerhaften Anmeldungen) zurücksetzen
- Passwörter administrativ neu setzen
- Kein Ablaufdatum des AMPR-AD-Account Passworts

Berechtigungen für LDAP:

- Analog zu Windows AD

Berechtigung für SAP:

- Der Account muss berechtigt sein, die folgenden BAPIs ausführen zu dürfen:
    - BAPI_USER_GETLIST
      BAPI_USER_GET_DETAIL
      um Benutzerdetails (z.B. Sync oder gesetzte Locks) abzurufen
    - SUSR_LOGIN_CHECK_RFC
      um ein Passwort zu prüfen
    - BAPI_USER_CHANGE
      um ein Passwort (administrativ) zurück zu setzen
    - SUSR_USER_CHANGE_PASSWORD_RFC
      um ein Passwort (im Benutzer-Kontext) zu ändern
    - BAPI_USER_UNLOCK
      um einen Account zu entsperren

2.5 SMTP-Gateway

AMPR wird Emails über Ihren konfigurierten Mailserver versenden. Dabei werden sowohl ungeschützte als auch SSL-geschützte Verbindungen unterstützt, ebenso wie eine eventuell erforderliche Authentifizierung.

2.6 Firewall & offene Ports

Die Web-Komponenten von AMPR und der AMPR Server müssen sowohl untereinander als auch mit den Zielsystemen, dem Active Directory / LDAP und der Datenbank kommunizieren. Dafür sind ggf. Ausnahmeregeln in Ihrer Firewall zu definieren sowie bestimmte Ports für die beteiligten Server zu öffnen. Die Clients benötigen in aller Regel keine Anpassungen.

2.6.1 Webserver

Der für die Websites konfigurierte Port muss offen sein, d.h. in der Regel Port 80 oder 8080 bzw. 443 oder 8443 für HTTP bzw. HTTPS. Es empfiehlt sich, HTTPS zu verwenden.

2.6.2 Active Directory / LDAP

Die für das AD zu öffnenden Ports können sich je nach verwendetem Server-Betriebssystem unterscheiden. Eine vollständige Übersicht finden Sie unter https://technet.microsoft.com/en-us/library/dd772723%28v=ws.10%29.aspx (letzte Prüfung: 20.09.2023). Für den LDAPS Zugriff muss der Port 636 (Standard / Default) geöffnet sein.

2.6.3 Datenbank

Sofern Sie eine Standardinstallation der MS SQL Server Datenbank verwenden, muss der Port 1433 geöffnet sein, andernfalls öffnen Sie den von Ihnen konfigurierten Port.

2.7 Datenbank

Es wird eine leere Datenbank (Namensvorschlag: `AMPRDB`) auf MS SQL Server 2016 oder höher benötigt. Das DBMS muss die Kommunikation über TCP/IP erlauben. Der Account, den AMPR für den DB-Zugriff verwenden soll, muss bereits auf dem DBMS eingerichtet sein und die Rolle *db_owner* erhalten (für die AMPR DB). Es hat sich bewährt, den Account als Datenbank-User einzurichten (das DBMS überprüft das PW) statt einer Windows-Authentifizierung.

Stellen Sie sicher, dass sowohl die Instanz als auch die angelegte Datenbank die Sortierung (Collation) „Latin1_General_CI_AS“ verwenden. Da diese im Nachhinein für eine Instanz nur schwer verändert werden kann, erstellen Sie ggf. eine eigene Instanz für die AMPR Datenbank.
