
Tekniska förutsättningar för Amido Alliera

Avser Amido Alliera 3.6.
Copyright © 2011-2019 Amido AB

Innehållsförteckning

1. Introduktion	1
2. Systemkrav	1
2.1. Plattformer	1
2.2. Kapacitetskrav	1
2.3. Utrymmeskrav	2
2.4. Klienter	2
2.5. Övrigt	2
3. Förutsättningar för installation	3
3.1. Användarkonton för tjänster	3
3.2. Intern kommunikation	3
3.3. Kommunikation med klienter	3
3.4. Kommunikation med externa system	4

1. Introduktion

Amido Alliera är huvudsakligen utvecklat i Microsoft .Net och körs på en Windowsplattform. Som egen databas används Microsoft SQL Server. Kraven för system anslutna till Alliera varierar per system.

Alliera består huvudsakligen av:

- Ett antal komponenter som installeras som tjänster i Windows.
- Två webbapplikationer (de flesta användare kommer bara i kontakt med den ena).
- Två databaser.

2. Systemkrav

2.1. Plattformer

För nyinstallation av Alliera rekommenderas en miljö enligt följande:

- Microsoft Windows 2012 R2 eller senare. .Net 3.5 samt 4.7.2 (eller senare) ska vara installerat, samt IIS.
- Microsoft SQL Server 2012 R2 eller senare.

Stöd för Windows 2008 R2 och SQL Server 2008 R2 kommer att fasas ut under 2019.

2.2. Kapacitetskrav

Många installationer klarar sig på 2 cpu-kärnor och 4GB RAM på applikationsservern om denna används enbart för Alliera (inklusive SQL Server).

Om man har fler än 20000 personer/lägenheter i databasen och fler än 20 samtidigt aktiva användare så kan det vara aktuellt att dubbla antalet cpu-kärnor och RAM, alternativt att köra SQL Server på en separat maskin.

2.3. Utrymmeskrav

Allieras installationsfiler behöver normalt 500-1000 MB diskutrymme, men vi rekommenderar att man avsätter minst 10 GB diskutrymme för smidig hantering vid uppgradering samt utrymme för loggfiler (intressanta vid felsökning).

Allieras primärdatas kräver ca 3GB i en installation som omfattar ca 2500 behörigheter, 50000 personer/lägenheter, 60000 passerkort och 250000 behörighetstilldelningar. En liten installation med ca 2000 personer/lägenheter kan kräva ca 500MB. Vi rekommenderar att man avsätter diskutrymme motsvarande minst 5 gånger det förväntade behovet. I synnerhet i samband med driftsättning kan extra utrymme krävas.

Alliera händelsedatabas kräver mer utrymme, i synnerhet ifall händelser från passersystemen också importeras till Alliera. Exempel:

- En liten installationen med ca 2000 personer/lägenheter som sparar händelser i 12 månader har genererat ca 3,5 miljoner händelser och kräver ca 5GB.
- En stor installation med ca 30000 personer som sparar händelser i 24 månader har genererat ca 280 miljoner händelser och kräver ca 80GB.

Vi rekommenderar att man avsätter diskutrymme motsvarande minst 2 gånger det förväntade behovet.



Notera

Uppskattning av utrymmeskrav för databaser är alltid vanskligt eftersom det beror mycket på antalet poster i databasen, men också på användningsmönster.

2.4. Klienter

Användarna kommer i kontakt med Alliera genom ett webbgränssnitt. Webbgränssnittet använder moderna och standardiserade webbt tekniker (HTML5). Det förekommer inga plugins eller Java. Som webbläsare rekommenderas någon av följande (andra moderna webbläsare kan fungera):

- Senaste versionen av Chrome eller Firefox.
- Internet Explorer 11 (ej stöd för webbkamera för fotoinläsning).
- Microsoft Edge.

För inläsning av passerkort utrustas klientstationerna vanligen med kortläsare som ansluts med USB. Dessa kortläsare emulerar ett tangentbord och kräver därför inga särskilda drivrutiner.

2.5. Övrigt

Alliera kräver inte generell åtkomst till Internet, men behöver kunna kommunicera med servrar för passersystem.

För att Amido ska kunna uppfylla åtaganden för support, underhåll och uppgraderingar krävs normalt att Amido har fjärråtkomst till aktuella servrar.

Alliera innehåller olika funktioner som kan skicka epost. För detta krävs tillgång till SMTP-server. Autentiserad SMTP kan användas om man vill.

Import/export av tabelldata till filer kan i dagsläget hantera CSV-filer (strävar efter att följa RFC4108) samt filer i formatet OOXML SpreadsheetML (XLSX).

3. Förutsättningar för installation

Amido rekommenderar i de flesta fall att samtliga Allieras komponenter körs på en och samma server. Undantaget är databaserna som kan ligga på samma eller separat server (beroende på önskemål och installationens storlek).

Det är också möjligt att installera Allieras komponent för ett visst passersystem direkt på den server som kör det aktuella passersystemet. Detta kan vara intressant ifall det aktuella passersystemet har begränsningar som gör det svårt att anropa det direkt över nätverk. Nackdelen är att uppgradering av Alliera blir något krångligare.

Det är oftast rekommenderat att köra Alliera på en server som inte används till annat. På rent tekniska grunder så kan Alliera vanligen samsas med andra mjukvaror på samma server, men av praktiska skäl brukar det vara enklast med en separat server. Amidos tekniker behöver vara lokala administratörer på Allieraservern.

3.1. Användarkonton för tjänster

Allieras tjänster är avsedda att exekvera under dedikerade användarkonton. Om man kör Active Directory så rekommenderas att man för Alliera skapar två konton i AD. Ett som kör Allieras windowstjänster, och ett som kör webbapplikationerna. Om man saknar namngivningspolicy för användarkonton så föreslås namnet "AllieraSvc" respektive "AllieraWeb". Dessa konton ska endast användas av Alliera, inte av andra mjukvaror eller personer.

Om man inte kör Active Directory så kan Alliera istället exekvera under konton som skapats lokalt på Allieraservern.



Notera

Notera att ifall Active Directory inte används så *måste samtliga* Allieras tjänster köras på samma server. Undantaget är webbgränssnittet som kan konfigureras för en "delad" installation där webbgränssnittet, om man vill, körs på en webbserver utanför Active Directory.

Databaserna kan ligga på separat server ifall SQL Server-autentisering används.

3.2. Intern kommunikation

Allieras komponenter kommunicerar med varandra genom HTTP-baserade webbservices på *valfri port, vanligen port 9500*. Komponenterna autentiserar mot varandra genom Windowsautentisering för att undvika lösenord i konfigurationsfiler. Undantaget är webbgränssnittet som kan konfigureras för en "delad" installation där webbgränssnittet, om man vill, körs på en webbserver utanför Active Directory.

Det konto som Alliera exekverar under måste ges tillåtelse att använda aktuell URL på servern. Detta hanteras normalt av Amidos tekniker vid installation.

Alliera ansluter mot SQL Server via TCP enligt den konfiguration som angetts. Om SQL Server ligger på samma maskin som Alliera, eller om Alliera exekverar under AD-konton, så rekommenderas att man använder Windowsautentisering även mot databaserna.

3.3. Kommunikation med klienter

Användarna anropar webbapplikationerna över HTTP eller HTTPS, normalt på respektive protokolls standardport.

3.4. Kommunikation med externa system

Kommunikation med passersystem (vanligen respektive systems serverinstallation) och andra typer av externa system sker på olika sätt beroende på fabrikat. Nedan följer en redogörelse för de vanligaste.

3.4.1. Aptus MultiAccess

Alliera ansluter direkt till systemets databas i SQL Server. Windowsautentisering rekommenderas om möjligt.

3.4.2. ASSA ARX

Alliera ansluter till ARX-servern på dess port TCP 5003 med protokoll HTTPS. Autentisering sker med konto i ARX. Det rekommenderas att ett dedikerat konto "ALLIERA" skapas i ARX.

3.4.3. Axema

Alliera ansluter till Axemas produkter via deras API.

3.4.4. Dinbox

Alliera ansluter till Dinbox REST-baserade API (HTTPS).

3.4.5. RCO R-Card M5

Alliera ansluter direkt till systemets databas i SQL Server. Windowsautentisering rekommenderas om möjligt.

Alliera behöver också ansluta till RCO M5:s komponent "RaServer" på M5-servern. Denna kommunikation sker via DCOM. Autentisering sker med konto i M5. Det rekommenderas att ett dedikerat konto "ALLIERA" skapas i M5 (fullständiga rättigheter).

En klientinstallation av RCO M5 måste finnas på Allieras server. Denna ska vara av samma version som M5-servern.

3.4.6. iLOQ

Alliera ansluter till iLOQs REST-baserade API (HTTPS).

3.4.7. Bravida Integra

Alliera ansluter till Integras API (webservice). För vissa begränsade funktioner används direkt kommunikation med Integras databaser i MS SQL Server.

3.4.8. Stanley SSM

Alliera läser från SSMs databaser i MS SQL Server, och skriver ändringar till SSM via det systemets dokumenterade importdatabas "MultiMaxImport".

3.4.9. Vanderbilt Omnis 2010 (fd. Bewator)

Alliera ansluter till Omnis server med dedikerat protokoll på TCP port 4006. Autentisering sker med identifieringsnyckel skapad i Omnis.

3.4.10. Vanderbilt Entro (fd. Bewator)

Alliera ansluter direkt till Entro-central genom protokollet BAPSI. Autentisering sker med identifieringsnyckel skapad i Entro-programmet.

3.4.11. Traka32

Alliera ansluter direkt till systemets databas i SQL Server enligt dokumenterat integrationsprotokoll. Windowsautentisering rekommenderas om möjligt.

3.4.12. Traka Web

Alliera ansluter till Traka Web Integration Engine (REST/HTTPS).

3.4.13. Salto

Alliera kommunicerar med Salto via dess "User Sync Staging Table", kompletterad med läsning via SQL.

3.4.14. Tidomat PW32

Alliera anropar Tidomats protokoll "SafeAPI" (web service), med viss komplettering genom direkt läsning med SQL.

3.4.15. ProAcess

Alliera kommunicerar med ProAcess genom att exekvera ProAcess verktyg för export/import till och från XML. En klieninstallation av ProAcess måste finnas på Allieraservern.

3.4.16. Pacom Unison

Alliera anropar Unison genom dess API "Unison Access Service API" (web service).

3.4.17. Microsoft Exchange

Alliera ansluter över protokollet "Exchange Web Services".

3.4.18. Microsoft Active Directory

Alliera kan integreras mot Active Directory på två olika sätt, för olika syften.

Autentisering av inloggning till Alliera

Alliera använder normalt Windowsautentisering mot lokalt konto eller Active Directory för autentisering mellan Allieras komponenter.

Allieras webbgränssnitt kan konfigureras för att autentisera användare mot konton i Windows eller Active Directory. För detta används Windows standardprotokoll.

Import av information till kortägare

Alliera kan ansluta till Active Directory och löpande importera utvalda delar av katalogen som kortägare, som sedan i Alliera kan tilldelas passerkort och behörigheter.

Denna anslutning mot Active Directory använder LDAP.