CRM & ERP ECM FINANCE BI eBUSINESS COLLAB HOSTING

mySTEPS Technologie

Informationen für Administratoren

Version: 1.0
Stand: 17.09.2018
Ansprechpartner: Produktmanagement Step Ahead AG

WWW.STEPAHEAD.DE | .AT | .CH

Inhaltsverzeichnis

1 Über mySTEPS

Die Step Ahead AG begleitet als „Digitalisierungsratgeber“ ihre mittelständischen Kunden auf dem Weg zum digitalen Unternehmen. mySTEPS ist dabei eine digitale Arbeitsplatzlösung, die jeden Mitarbeiter mobil mit Informationen aus Steps Business Solution | STEPS.IT | LS BIZ versorgt - und das geräteunabhängig, zu jeder Zeit, an jedem Ort. Ziel ist es, die Suche nach Informationen und Kontakten zu reduzieren und souveränes Agieren vor Ort zu ermöglichen.

2 Was ist die Steps CRM-API?

Die Steps CRM-API ist ein mySTEPS Bestandteil, der einem Gateway zur Cloud-Synchronisation den Zugriff auf bestimmte Daten der ERP-Lösung über einen REST WebService ermöglicht. Das Gateway hat auch die Aufgabe, die Daten aus einem Hersteller-spezifischen Format in das weit verbreitete CDM (Common Data Model)[i] zu überführen und in der Cloud zu speichern.

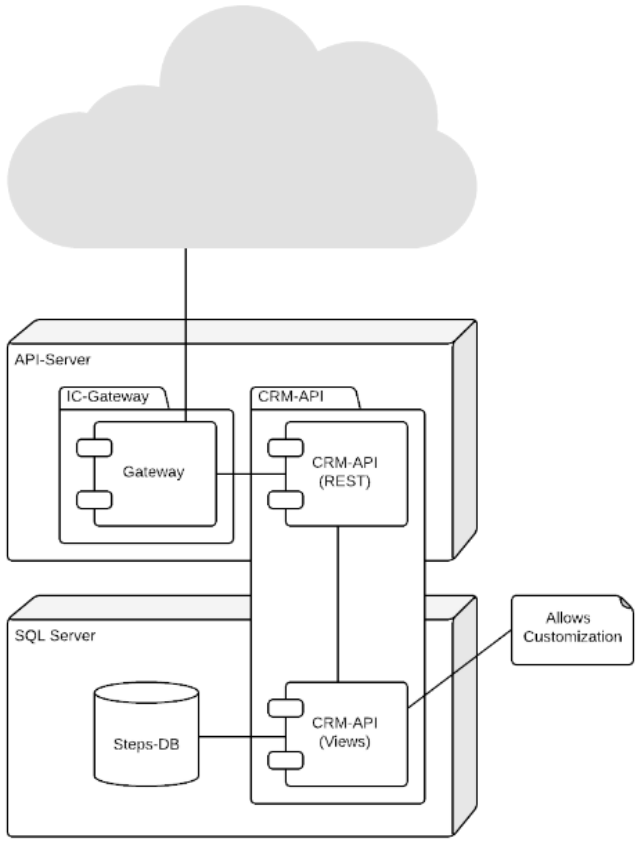

Abbildung 1: Deployment-Diagramm der Steps CRM-API

Im Folgenden werden die einzelnen technologischen Komponenten erläutert, die bei der STEPS CRM-API zum Einsatz kommen und damit einen stabilen, sicheren und zukünftig leicht skalierbaren Betrieb ermöglichen.

3 Technologische Basis im Überblick

Die Steps CRM-API setzt auf die neuesten von Microsoft empfohlenen Technologien wie ASP.NET Core, Entity Framework Core und OData auf. In Zukunft ermöglicht dieser technologische Rahmen einen flexiblen Einsatz in heterogenen IT-Landschaften. Wir gehen davon aus, dass dies zunehmend zum Standard in einer Industry 4.0 geprägten Welt wird.

Mehr Informationen dazu sind z.B. auf
http://docs.microsoft.com/en-us/aspnet/core/ zu finden.

3.1 ASP.NET Core

ASP.NET Core ist ein von Microsoft gefördertes Open Source Framework zum Entwickeln von modernen Cloud-Anwendungen in Cross-Plattform und High-Performance Szenarien. Darauf aufsetzende Applikationen laufen im einfachsten Fall als standalone Konsole-Anwendung im leichtgewichtigen self-hosting Modus.

Die technologische Grundlage bietet ein Mini-Webserver namens Kestrel. Ein derartig fokussierter Webserver befreit den Administrator vor der aufwendigen Installation, Konfiguration und Pflege von Schwergewichten wie beispielsweise IIS.

In komplexen Einsatzbereichen können typische schwergewichtige Webserver wie IIS, Apache oder Nginx vorgeschaltet werden, um fortgeschrittene Workflows und Prozesse (Load Balancing, Reverse Proxy, Redirecting, Rewriting) zu etablieren.

3.2 Entity Framework Core

Wie ASP.NET Core ist auch das Entity Framework Core (EF Core) ein von Microsoft gefördertes Open Source Framework für Cross-Plattform-Szenarien. Es dient als sogenannter O/R-Mapper (Object Relational Mapper) für einen abstrahierten Datenzugriff. Der Entwickler muss sich so nicht mehr im Detail um die aufwändigen und fehleranfälligen Konstrukte zum Lesen und Schreiben von Daten kümmern.

Durch die am Markt verfügbaren EF-Core Provider für die unterschiedlichsten Datenbanksysteme und Betriebssysteme (SQL Server, Oracle, PostgreSQL, Db2, Linux, usw.) kann flexibel auf die bei Ihnen vorliegende Lizenzsituation eingegangen werden. Der Vollständigkeit halber ist zu erwähnen, dass zurzeit die STEP Ahead ERP-Lösungen nur auf MS SQL Server unter Windows lauffähig sind.

3.3 ODATA

Das Open Data Protocol (OData) ist ein von Microsoft initiiertes offenes Protokoll, das die Erstellung und Verwendung von abfragbaren und interoperablen RESTful-APIs auf einfache und standardisierte Weise ermöglicht. Mit OData erstellte und verwendete REST-APIs unterstützen Web-Clients, Ressourcen zu veröffentlichen und zu bearbeiten, die mithilfe von URLs identifiziert und in einem Datenmodell mithilfe einfacher HTTP-Nachrichten definiert werden. Diese API-Funktionalitäten wird die Step Ahead AG zukünftig auch Partnern und externen Entwicklern bereitstellen.

4 Höchstmögliche Sicherheit

mySTEPS bietet die höchstmögliche Sicherheit gegen Datenraub und -missbrauch sowie gegen Angriffe von außen durch

- verschlüsselte Daten-Transporte
- abgesicherte Daten-Endpunkte
- die Durchsetzung von Berechtigungen im Daten-Zugriff.

Erreicht wird dies durch

- die Verwendung von HTTPS
- geringstmögliche Verwendung von Ports und deren freie Zuweisung
- ein klares Regelwerk der Inbound- & Outbound-Kommunikation
- API-Key- bzw. Token-basierte Berechtigung
- Verwendung von dedizierten Accounts für Installation und Services.

4.1 Verwendung von HTTPS

Gemäß heute empfohlener und üblicher Prinzipien erfolgt die Kommunikation mit den REST-Endpoints vorzugsweise über HTTPS. Ein entsprechendes Zertifikat kann kostenlos über den Anbieter Let's Encrypt (https://letsencrypt.org) bezogen werden. Wir empfehlen, dieses vorab einzuspielende Zertifikat im Installationsprozess auszuwählen und zur Verwendung vorzusehen.

4.2 Verwendung von Ports & freie Zuweisung

Standardmäßig wird die Steps CRM-API auf Port 49152 installiert. Das ist der erste Port aus dem Bereich der private Ports (bis 65535). Gerade in Reverse Proxy Szenarien empfiehlt es sich, einen zufälligen Port aus diesem Bereich zu wählen, um den Angriffsvektor gegen typische Portnummern zu entschärfen.

4.3 Firewall-Rules für Inbound- & Outbound-Kommunikation

- **CRM-API und Gateway auf dem gleichen Server, On-Premises**
  Im o.g. typischen Auslegungsfall werden die STEPS CRM-API und das Gateway auf dem gleichen Server und On-Premises betrieben. In diesem Fall muss lediglich die Site-Firewall für ausgehenden Traffic auf die Azure Services geöffnet werden. Im Allgemeinen dürfte dieser Traffic nicht reglementiert sein und keinen Eingriff erfordern.
- **Steps CRM-API und Gateway auf unterschiedlichen Servern, beide On-Premises**
  Für die Site-Firewall gelten die gleichen wie im anderen On-Premises-Szenario genannten Bedingungen. Zusätzlich muss jedoch die lokale Firewall Incoming-Traffic für den Port erlauben, welcher während der Installation definiert wurde.
- **On-Premises Steps CRM-API und Gateway in der Cloud**
  Dieses Szenario wird von uns nur empfohlen, wenn ein professioneller Webserver vorgeschaltet wird, da der Mini-Webserver Kestrel derzeit über keinerlei Funktionalitäten verfügt, DoS und ähnliche Attacken zu identifizieren und einzudämmen bzw. zu blockieren. Zusätzlich müssen sowohl die lokale als auch die Site-Firewall einen Incoming-Traffic für den Port erlauben, welcher während der Installation definiert wurde. Weiterführende Informationen finden sich in der Microsoft Dokumentation zu ASP.NET Core http://docs.microsoft.com/en-us/aspnet/core/host-and-deploy.

4.4 API-Key- bzw. Token-basierte Berechtigung

Während der Installation wird ein zufälliger API-Key erzeugt, mittels welchem das Gateway über einen Authentifizierungs-Endpunkt einen Token anfordern kann. Dieses Token ist 24 Stunden gültig. Durch die Trennung in API-Key und Token ist es möglich die Zugriffe auf die Steps CRM-API bzgl. der Konsumenten individuell über das jeweilige Token zu protokollieren.
Ein kompromittierter API-Key kann jederzeit neu vergeben werden. Dazu ist entweder in der Datei appsettings.json der API-Key zu ändern oder die Instanz der Steps CRM-API zu deinstallieren und neu zu installieren. In beiden Fällen muss im Gateway über das Admin-Werkzeug der neue API-Key hinterlegt werden.

4.5 Accounts für Installation und Services

Während der Installation werden Schreibberechtigungen auf die ERP-Datenbank benötigt, um die Views einzuspielen. Im späteren Einsatz wird nur noch ein Lesezugriff benötigt. Diese Trennung von Verantwortlichkeiten wurde schon für den Installationsprozess berücksichtigt. Mittels eines temporären Installations-Accounts mit administrativer und hochgestuften Berechtigung für

- den Server, auf welchen die Steps CRM-API installiert wird
- die ERP-Datenbank

erfolgt die Installation der Steps CRM-API und das Einspielen der Views. Dieser Account kann im Abschluss deaktiviert werden. Dadurch wird ein unberechtigter Zugriff auf die ERP-Datenbank schon im Ansatz ausgeschlossen.

Während der Installation kann dann ein dedizierter Service-Account spezifiziert werden, unter dessen Kontext die Steps CRM-API am Anschluss läuft. Dieser Service-User sollte nur eingeschränkte Berechtigung erhalten

- auf den Server, auf welchem die STEPS CRM-API läuft (u.a. keine interaktive Login-Berechtigung)
- auf die Datenbank (nur lesender Zugriff)

Diese strikte Trennung der Verantwortlichkeiten und Berechtigungsvergabe orientiert sich an üblichen Best Practices in der IT.

5 Deployment-Empfehlung

In einer zunehmend modularisierten und von Microservices geprägten IT-Welt ist es von grundlegender Bedeutung, die unterschiedlichsten Deployment-Szenarien zu erlauben.

Dementsprechend sind die beiden primären Dienste des Infocenters - die Steps CRM-API und das Gateway - auch sehr individuell installierbar, mit Skalierbarkeit zwischen On-Premises und Cloud.

Aufgrund der Datenmengen, welche zwischen Steps CRM-API und Gateway ausgetauscht werden und der Interaktion zwischen ihnen, empfiehlt es sich, beide Services auf dem gleichen Server zu installieren. Dieser Server sollte wiederrum mit möglichst hoher Bandbreite mit dem SQL Server mit der ERP-Datenbank in Verbindung stehen.

Je nach Auslegung des SQL Servers und dessen freien Kapazitäten können die beiden Services auch auf ihm installiert werden. Dies empfehlen wir aber nur in genau skizzierten und abgesprochenen Anwendungsfällen, da während der Datensynchronisation die Steps CRM-API und das Gateway einen gewissen Ressourcen-Anspruch haben und das zu Lasten der SQL Server Performance geht. Abhängig von den gewünschten Synchronisierungsintervallen (bspw. nur "nachts") und der Verwendung des SQL-Servers (nur "tagsüber") kann dies aber eine kostenschonende Deployment-Variante sein.

6 Installationsvorgehen

Derzeit werden die Steps CRM-API und das IC-Gateway über zwei eigene Installer ausgeliefert. In zukünftigen Versionen werden sie Bestandteil der ERP-Lösung bzw. mySTEPS sein.

7 Customizing für die Anzeige kundenspezifischer Daten

mySTEPS kann Informationen anzeigen, welche nicht in der Standardauslieferung von Steps Business Solution | STEPS.IT | LS BIZ enthalten sind (u.a. Mitarbeiter-Anzahl, Business-Kategorisierung). Für beim Kunden angepasste Felder wird ein Customizing des Datenlese-Vorgangs über Views erlaubt. Ohne Anpassung liefern diese Views leere Daten über die Steps CRM-API. Durch das Aufbereiten der durch Customizing erfassten Daten, können die Views die gewünschten Informationen liefern.

[i] Im Common Data Model (CDM) werden Daten in der Cloud zur Anzeige in mySTEPS vorgehalten. Es definiert Standard-Entitäten, welche häufig verwendete Konzepte und Aktivitäten in Geschäftsanwendungen repräsentieren. Beispielsweise umfasst es klar definierte, modulare und erweiterbare Geschäftseinheiten wie Geschäftspartner, Geschäftseinheit, Kontakt, Lead, Opportunity und Produkt sowie Interaktionen mit Lieferanten, Mitarbeitern und Kunden.