

Integration eIAM in AWS Cognito

Datum: 17.05.2021

Autor: Dominic Rohner (dominic.rohner@swisstopo.ch)

Inhalt

Einführung	1
Erstellung AWS Cognito User Pool	1
Einstellungen AWS Cognito User Pool	2
eIAM als Identity Provider hinzufügen	2

Einführung

Mit Amazon Cognito kann die Registrierung und Anmeldung von Benutzern und die Zugriffskontrolle von Web- und mobilen Anwendungen hinzugefügt werden. Cognito kann für Millionen von Benutzern skaliert werden und unterstützt die Anmeldung durch soziale Identity Providers wie Apple, Facebook, Google und Amazon oder Unternehmens-Identity Provider über SAML 2.0 und OpenID Connect.

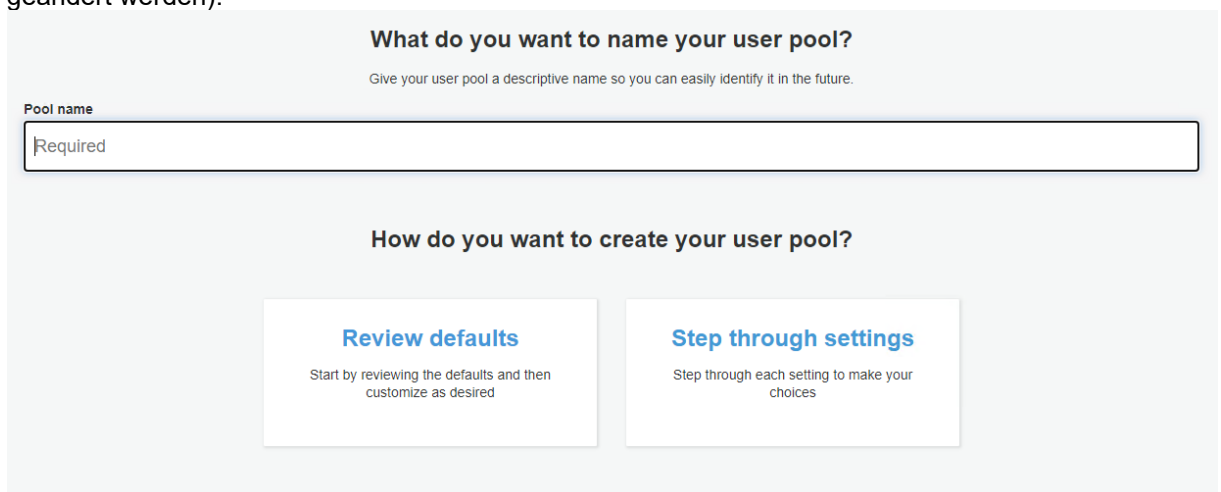
eIAM kann über SAML oder OIDC als Identity Provider hinzugefügt werden. Anschliessend muss ein Mapping zwischen den User Pool Attributen und der SAML/OIDC Attributen gemacht werden. In Cognito wird bei einem Login über eIAM automatisch für den Benutzer ein User angelegt. Es können auch Gruppen angelegt werden, welche dann die Berechtigungen regeln.

Erstellung AWS Cognito User Pool

Die Voraussetzung ist ein AWS Account, in welchem man die Berechtigungen hat um im Service «Cognito» Ressourcen anzulegen.

Vorgehen:

1. Auswählen des Service «Cognito»
2. «Manage user pools»
3. «Create a user pool»
4. Namen setzen und «Review defaults» auswählen (die Einstellungen können später auch noch geändert werden):



5. «Create pool», anschliessend wird der Pool erstellt

Einstellungen AWS Cognito User Pool


In einem Cognito User Pool können diverse Einstellungen vorgenommen werden:

<div><div>General settings</div><div>Users and groups</div><div>Attributes</div><div>Policies</div><div>MFA and verifications</div><div>Advanced security</div><div>Message customizations</div><div>Tags</div><div>Devices</div><div>App clients</div><div>Triggers</div><div>Analytics</div></div>	<div></div>
<div><div>App integration</div><div>App client settings</div><div>Domain name</div><div>UI customization</div><div>Resource servers</div></div>	<div>Einstellungen betreffend der Benutzer</div> <div>Unter «Users and groups» können die Benutzer Gruppen zugeteilt werden. Unter «Attributes» können die Standard Attribute eines Benutzers festgelegt werden, welche später mit den SAML/OIDC Attributen gemappt werden. Die restlichen Einstellungen sind nur dann interessant, wenn über Cognito auch Benutzer angelegt werden.</div>
<div><div>Federation</div><div>Identity providers</div><div>Attribute mapping</div></div>	<div>Einstellungen betreffend der Applikation</div> <div>Unter «App client Settings» wird festgelegt mit welchen Möglichkeiten man sich über Cognito einloggen darf. Die restlichen Einstellungen dienen zur UI Anpassung.</div> <div>Einstellungen für Identity Providers</div> <div>Unter «Identity providers» werden IdPs wie eIAM hinzugefügt und unter «Attribute Mapping» werden die SAML/OIDC Attribute mit den Cognito Attributen verbunden.</div>

eIAM als Identity Provider hinzufügen

Unter «Federation» → «Identity provider» kann eIAM als IdP hinzugefügt werden.

Dazu die XML-Datei der eIAM Integration unter SAML hochladen, einen Namen setzen und mit «Create provider» den Provider erstellen:



SAML

You can use a corporate identity provider to sign in users through SAML federation.

[Learn more about SAML.](#)

Metadata document

SAML.xml

Provider name

eIAM

Identifiers (optional)

☐ Enable IdP sign out flow

Create provider

Anschliessend werden unter «Attribute mapping» die Attribute miteinander verbunden:

eIAM

Capture	SAML attribute	User pool attribute
<input checked="" type="checkbox"/>	<div>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</div>	<div>Email</div> <div></div>

Add SAML attribute