AMAZON COGNITO: AUTENTICAZIONE GESTITA MEDIANTE SINGLE SIGN-ON

Amazon API Gateway | Amazon Cognito | DevOps | How-to | Multi-Factor Authentication | Single-Sign-On (SSO)

beSharp | 23 Agosto 2019

Una delle features più ricorrenti nelle applicazioni web e mobile è certamente l'autenticazione degli utenti; poter fare off-load delle responsabilità connesse alla gestione dell'autenticazione degli utenti aumenta notevolmente la robustezza delle soluzioni realizzate e la velocità di sviluppo.

L'utilizzo dei managed services permette al team di sviluppo di automatizzare e rendere robuste alcune funzionalità critiche nella realizzazione di applicazioni web come ad esempio la user authentication. Il managed services dedicato alla risoluzione di questo aspetto è **Amazon Cognito**.

Amazon Cognito fornisce un building-block in grado di accelerare e rendere sicuro il processo di autenticazione ed autorizzazione degli utenti verso applicazioni mobile o web.

Prima di entrare nel vivo della trattazione è utile definire i termini specifici del servizio e i concetti propedeutici alla comprensione dei temi trattati.

Cos'è Amazon Cognito?

Amazon Cognito consente di aggiungere strumenti di registrazione e autenticazione ad applicazioni Web e mobile. Permette di autenticare gli utenti sia mediante una user pool completamente gestita sia tramite un provider di identità esterno (IdP). Inoltre può fornire credenziali di sicurezza temporanee per accedere alle risorse AWS.

Amazon Cognito è compatibile con provider di identità esterni che supportino lo standard SAML o **OpenID** Connect, con provider di identità social quali **Facebook**, **Twitter** e **Amazon** e consente anche di integrare il proprio provider di identità.

Amazon Cognito è un servizio distribuito e ad accesso pubblico; ciò significa che chiunque può chiamare le API di Cognito per autenticarsi presso un servizio. Si tratta di un comportamento

standard e ben rodato; è normale che un servizio di autenticazione sia pubblico ed accessibile per consentire ai client di effettuare le operazioni di login.

La sicurezza della soluzione è garantita da Amazon, che gestisce completamente il servizio e le API accessibili dal pubblico.

I client possono quindi effettuare il login mediante uno degli IdP supportati, oppure inviare a Cognito username e password per ottenere in cambio un **token di identità** e, opzionalmente, un set di credenziali IAM la cui policy è controllata da Cognito mediante apposite configurazioni.

I client in possesso del token di identità possono autenticarsi presso i servizi che usano Amazon Cognito come IdP e potranno usare le chiavi IAM (se fornite) sia per chiamare il back-end applicativo che supporta la IAM authentication, sia per accedere direttamente alle risorse sull'account AWS consentite da apposite policy.

Amazon Cognito **si integra con API Gateway in modo automatico,** permettendo quindi di proteggere i back-end in modo completamente gestito ed automatico.

I back-end protetti da API Gateway e Cognito non riceveranno richieste che non superino i controlli di autenticazione, permettendo di ottenere una soluzione più robusta e cost efficient.

L'integrazione tra Amazon Cognito e API Gateway permette di implementare solo l'autenticazione oppure autenticazione ed autorizzazione.

Nel caso in cui si intenda sviluppare la sola autenticazione sarà possibile sfruttare **l'integrazione mediante Cognito User Pool**, che garantirà l'accesso alle API a qualsiasi utente correttamente autenticato mediante credenziali o tramite IdP esterno.

Se si seleziona **l'integrazione con IAM** si potranno ottenere le funzionalità di autenticazione e autorizzazione. Verrà impiegato il token di identità di una User Pool per ottenere una coppia di chiavi IAM da utilizzare per effettuare le chiamate al back-end.

Diventa quindi possibile limitare i set di API accessibili a diversi gruppi di utenti. Inoltre, mediante le chiavi temporanee e le apposite policy gestite, è possibile dare accesso controllato e sicuro a subset di risorse AWS, permettendo ad esempio di caricare un file su S3 o di mettere un messaggio in una coda senza dover interagire con il back-end dell'applicazione.Di fatto si sta effettuando l'off-load di alcune operazioni in modo sicuro ed efficace.

Gli utenti vengono gestiti attraverso **due tipologie di pools,** che sono il fulcro del funzionamento di Amazon Cognito: **User Pools e Identity Pools.**

Andiamo quindi a descrivere i concetti principali di cognito.

User Pools

Un pool di utenti è una directory utenti configurabile per l'utilizzo con un'applicazione Web e/o mobile. Un pool di utenti consente di memorizzare in modo sicuro gli attributi del profilo dei tuoi

utenti.

Si tratta quindi di un modo per fare completo off-load della gestione degli utenti che decidono di registrarsi al servizio mediante username e password. Tra le operazioni di cui è possibile fare off-load della responsabilità vi sono certamente lo storage sicuro dei dati utente, la verifica di eventuali numeri di telefono o indirizzi email, la gestione delle API e del flusso di registrazione, login, logout e il reset password.

Le user pools sono un componente fondamentale di qualsiasi sistema di autenticazione basato su Amazon Cognito. È anche possibile collegare una user pool con un IdP esterno per permettere agli utenti del servizio di registrarsi ed accedere mediante Facebook, Google, amazon o qualsiasi IdP pubblico che supporti OpenID.

Identity Pools

I pool di identità sono container utilizzati da Cognito Identity per mantenere organizzate le identità federate dell'applicazione. Un pool di identità associa le identità federate provenienti da provider di identità esterni o User Pool con un identificatore utente specifico univoco. I pool di identità non memorizzano i profili degli utenti, ma solo il loro id univoco generato e gestito da Cognito. Un pool di identità può essere associato a una o più applicazioni.

Cognito Identity assegna agli utenti un set di credenziali temporanee e con privilegi limitati per accedere alle risorse AWS, perciò non è necessario usare le credenziali dell'account AWS per permettere agli utenti di interagire con le risorse cloud. Le autorizzazioni per ciascun utente sono controllate tramite ruoli di AWS IAM personalizzabili. È possibile definire regole per scegliere il ruolo IAM di ciascun utente; se utilizzi i gruppi in un pool di utenti Cognito, puoi assegnare ruoli IAM in base a tali gruppi. Cognito Identity consente inoltre di definire un ruolo IAM separato con permessi limitati per gli utenti guest privi di autenticazione. Infine, puoi usare identificatori univoci generati da Cognito per definire l'accesso degli utenti a risorse specifiche. Ad esempio, puoi creare una policy per un bucket S3 che permetta agli utenti l'accesso solo alla propria cartella.

Adesso che abbiamo definito tutti i concetti fondamentali possiamo passare alla parte centrale del nostro articolo, ovvero il **tutorial per configurare Amazon Cognito per consentire l'autenticazione degli utenti mediante la loro identità Google.**

Tutorial:

Il primo passo da portare a termine per la configurazione di Cognito è quello di creare una User Pool che andremo successivamente a federare con Google e con una Identity Pool al fine consentire agli utenti di identificarsi mediante Google e di ottenere un token di identificazione e una coppia di chiavi per accedere alle risorse cloud.

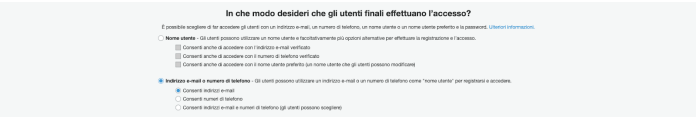
Creazione di uno User Pool

Dalla Console di Amazon, navigate all'interno della dashboard di Cognito e cliccate sul pulsante "Crea uno User Pool" per avviare il wizard di creazione.

Come prima cosa, ci verrà chiesto un nome per il nostro User Pool. A questo punto, possiamo decidere se proseguire con un wizard passo passo, o se creare uno User Pool con le opzioni di default e di revisionarlo prima della creazione. Scegliamo la prima opzione cliccando il pulsante "Esamina Impostazioni".

Il primo step del wizard ci permette di scegliere con quali informazioni gli utenti potranno effettuare il login su Cognito. Le opzioni sono molteplici: possiamo scegliere di far autenticare l'utente attraverso l'utilizzo di una username, di una mail, di un numero di telefono ecc... E' importante notare che queste possibilità valgono solo per quegli utenti che faranno login direttamente su cognito (dopo essersi registrati) e per quelli che utilizzeranno eventuali IdP esterni.

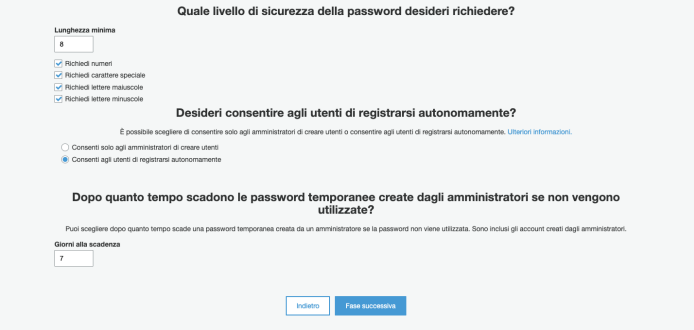
Per questo tutorial andiamo a selezionare "Indirizzo email o numero di telefono" e successivamente "Consenti indirizzi email" (Come da immagine). **In questo modo l'unica possibilità di login da parte degli utenti sarà utilizzando una email valida.**



A questo punto ci viene proposta la selezione degli attributi obbligatori in fase di registrazione dell'utente. Cognito mette a disposizione alcuni attributi standard quali nome, cognome, data di nascita e molti altri. Inoltre è possibile creare degli attributi custom che verranno salvati all'interno di cognito al momento della registrazione dell'utente. Per il nostro tutorial possiamo lasciare tutto come da default e passare al passo successivo.

In questo step è possibile configurare il livello di sicurezza a cui ogni utente che si registra alla nostra applicazione dovrà attenersi per creare una password sicura. Possiamo quindi inserire il limite minimo di caratteri della password e vari constraint sull'utilizzo obbligatorio di caratteri speciali, numeri, lettere maiuscole e lettere minuscole. Lasciamo i valori di default e proseguiamo con le altre configurazioni.

Il secondo e il terzo punto di questo step ci permettono di configurare la modalità di creazione degli utenti e la durata massima delle password temporanee generate dagli amministratori per i nuovi utenti che vengono creati. Sostanzialmente abbiamo due modi per poter creare gli utenti. Il primo consente agli utenti stessi di potersi registrare attraverso una pagina di registrazione, il secondo invece, prevede la creazione degli utenti mediante l'amministratore del sistema. Il che significa che sarà l'utente proprietario dell'applicazione, attraverso la Console di Amazon o attraverso la CLI, a creare l'utente con una password temporanea. Per il nostro tutorial selezioniamo la possibilità di poter far registrare gli utenti autonomamente (come da immagine) e proseguiamo cliccando il pulsante "Fase successiva".



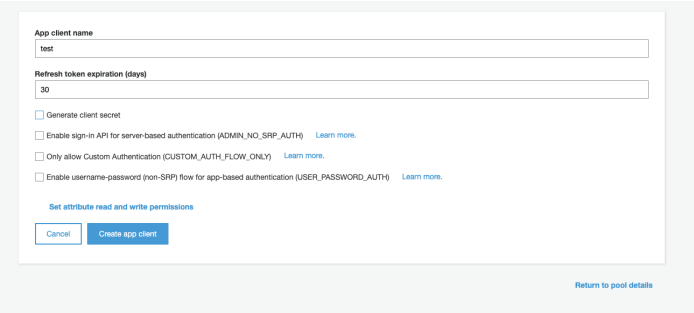
In questa parte del wizard possiamo andare ad **abilitare la Multi Factor Authentication** e, se vogliamo, la verifica della mail / telefono in fase di registrazione. Per il nostro tutorial possiamo lasciare l'MFA disabilitato e selezionare "e-mail" come attributo da verificare in caso di registrazione autonoma.

Nello step successivo, invece, è possibile andare a configurare tutti i messaggi automatici che saranno inviati da Cognito all'utente finale. Questi messaggi includono password temporanee e codici di verifica che possono essere inviati attraverso mail o attraverso SMS configurando Amazon SNS. Per il nostro tutorial possiamo lasciare tutto come da default e passare allo step successivo.

A questo punto del wizard possiamo aggiungere dei tag alla risorsa che stiamo andando a creare. Aggiungiamo i tag del caso o anche nessuno se si tratta di un esperimento e passiamo allo step successivo.

Ora ci viene chiesto se vogliamo che cognito salvi automaticamente i dispositivi in modo da non richiedere l'utilizzo della MFA ad ogni accesso. Dato che nello step precedente abbiamo lasciato la MFA disabilitata, selezioniamo "No" e proseguiamo allo step successivo.

Ci viene ora chiesto di creare un App Client che verrà poi utilizzato dalla nostra applicazione per poter effettuare le dovute chiamate di registrazione e login. Per farlo basterà schiacciare sul pulsante "aggiungi un client di app" , inserire un nome, rimuovere la spunta da "Genera segreto del client" e premere il pulsante "Crea client di app".



Possiamo quindi terminare il wizard andando a **creare il pool di utenti premendo il pulsante nell'ultima schermata.**

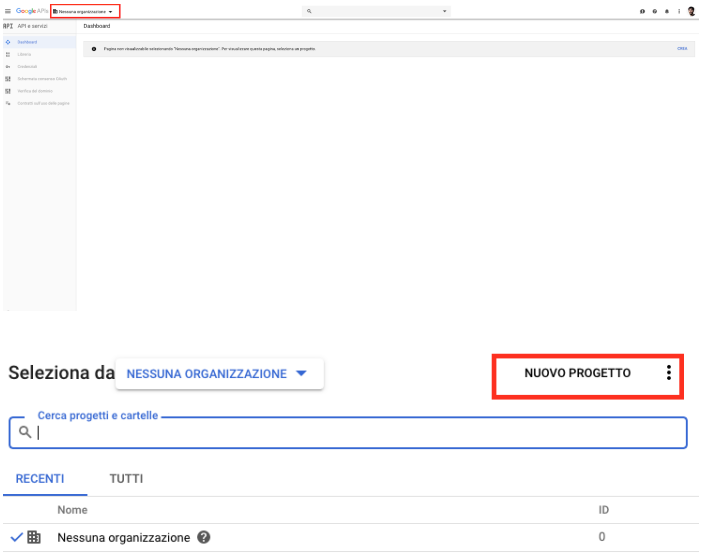
Prima di passare alle configurazioni per l'integrazione e scegliamo un nome di dominio per il nostro User Pool. Una volta scelto clicchiamo sul pulsante "Verifica disponibilità" e successivamente su "Salva modifiche".

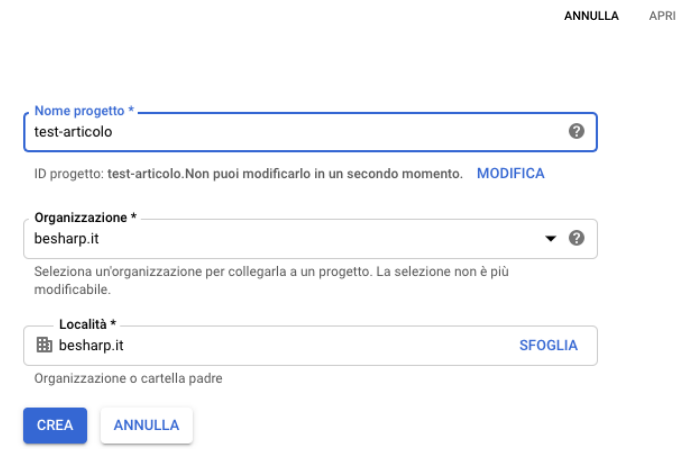
Configurazione Integrazione Identity Pool Esterno

Una volta creato lo user pool, possiamo passare all'integrazione con il nostro SSO. Per farlo

abbiamo bisogno di creare un **nuovo progetto dalla Google Developer Console** e ottenere delle credenziali di accesso. Una volta ottenute le credenziali passeremo alla configurazione di Cognito.

Rechiamoci sulla Google Developer Console e creiamo un nuovo progetto (come da immagini).

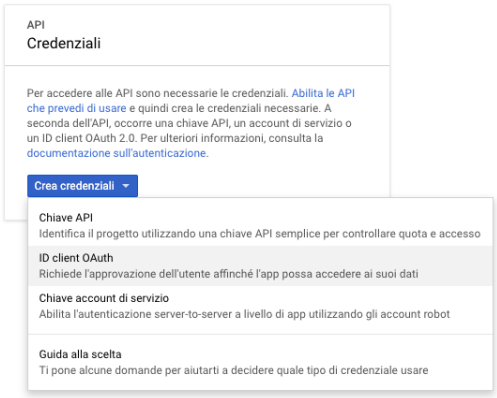




Una volta creato il nostro progetto, andiamo alla voce "Schermata consenso OAuth".

Qui andremo a configurare il nome dell'applicazione e andremo ad abilitare il dominio "amazoncognito.com". Per farlo basta inserirlo nell'apposito campo denominato "Domini autorizzati" e cliccare sul pulsante "Salva".

Rechiamoci ora sotto il campo "Credenziali" e clicchiamo sul pulsante "Crea credenziali" andando a selezionare "ID Client OAuth" dal menù a tendina proposto.

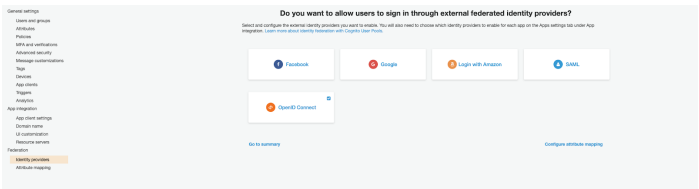


Selezioniamo poi “Applicazione web”, inseriamo un nome per il nostro client e **come origini javascript autorizzate andiamo ad inserire il nome di dominio del nostro Cognito User Pool** creato precedentemente (es: https://test-articolo.auth.eu-west-1.amazoncognito.com). Andiamo poi ad inserire lo stesso nome di dominio seguito da **/oauth2/idpresponse** all’interno del campo URI di reindirizzamento autorizzati (es: https://test-articolo.auth.eu-west-1.amazoncognito.com/oauth2/idpresponse) e premiamo il pulsante “Crea”.

A questo punto verrà visualizzato un popup contenente il nostro “ID Client” e il nostro “Client Secret”. **Copiamo i segreti in un file di testo per averli rapidamente disponibili in seguito.**

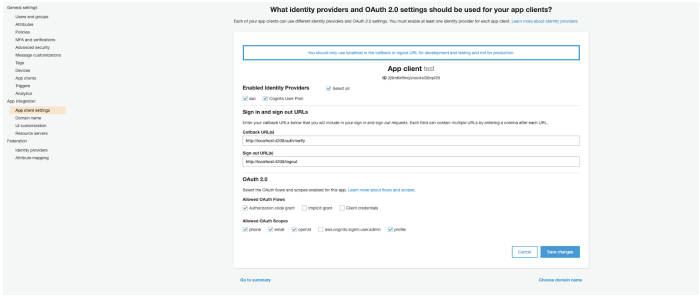
Passiamo adesso alla configurazione dell’integrazione tra i Cognito e Google cominciando da Amazon Cognito.

Navighiamo all’interno del menù “Provider di identità” e selezionare la tipologia di integrazione che vogliamo effettuare.



Da questo punto di vista, Amazon offre l’integrazione con i maggiori provider di identità tra cui Facebook, Google, Amazon e, più genericamente, tutti i provider che supportano i protocolli OpenId e SAML. Per questo tutorial andremo ad integrarci con Google. Per farlo clicchiamo il pulsante “Google” e andiamo ad inserire le informazioni dell’identity provider con quelle restituiteci durante la creazione del progetto Google.

L’ultimo passaggio rimanente, riguarda il linking delle due risorse create precedentemente. Per farlo, basta navigare all’interno della scheda “App client settings”. Nella schermata proposta bisognerà selezionare come Identity Provider il nostro identity provider creato precedentemente e fornire gli endpoint di callback come da immagine. Gli endpoint di callback saranno gli endpoint chiamati a fine autenticazione e conterranno il nostro token.



Per fare un test possiamo utilizzare l'Hosted UI fornita da Cognito navigando al dominio che abbiamo scelto precedentemente e passando come query string parameters il nostro client id, il redirect uri e alcune informazioni aggiuntive come da esempio:

https://test-articolo.auth.eu-west-1.amazoncognito.com/authorize?client_id=**{client-id}**&redirect_uri=http://localhost:4200/auth/verify&response_type=token

Una volta completato il processo di autenticazione, verremo automaticamente rediretti al nostro indirizzo di callback http://localhost:4200/auth/verify con la differenza che troveremo in query string parameter i nostri token di accesso.

A questo punto sta all'applicazione recuperare i token dalla chiamata di callback, che per lo scopo di questo tutorial abbiamo impostato a localhost, ed usarli per le successive chiamate al back-end.

Con questo tutorial abbiamo visto come configurare dall'inizio alla fine l'integrazione tra Amazon Cognito e Google. Abbiamo illustrato e testato come ottenere il token di identificazione e come usarlo per accedere ai servizi di back-end.

Restate sintonizzati per ricevere altri tutorial interessanti!

beSharp

Dal 2011 beSharp guida le aziende italiane sul Cloud. Dalla piccola impresa alla grande multinazionale, dal manifatturiero al terziario avanzato, aiutiamo le realtà più all'avanguardia a realizzare progetti innovativi in campo IT.

Get in touch

beSharp.it
proud2becloud@besharp.it