Federazione cross-account tra Amazon Connect e Azure AD con AWS SSO

26 Novembre 2021 - 5 min. read

Amazon Connect | *AWS Single Sign-On* | *Azure AD* | *cross-account federation* | *Identity Provider* | *Single-Sign-On (SSO)*

Per le aziende è diventato molto importante essere in grado di utilizzare differenti canali di comunicazione con i propri clienti, specialmente per fornire loro supporto.

Nel mercato dei servizi di contact center, in cui esistono già aziende affermate da tempo, Amazon Connect è una alternativa interessante da prendere in considerazione: è interamente gestito, facilmente scalabile e con un costo competitivorispettoai competitor sul mercato..

L'intelligenza artificiale abbinata agli algoritmi di machine learning rende possibile la sentiment analysis permettendo al business di ottenere informazioni di valore dai propri utenti.

Ogni cliente ha esigenze differenti che, a volte, ci portano a provare integrazioni tra servizi inusuali e non presenti nelle guide ufficiali.

In questo articolo descriveremo come siamo riusciti a configurazione una federazione cross-account fra Amazon Connect e Azure AD mediante l'uso di AWS SSO.

Use Case

Per un nostro cliente è emersa l'esigenza di configurare Amazon Connect affinché fosse possibile per gli utenti esistenti su Office365, contenuti quindi in una istanza

Azure Active Directory, autenticarsi. L'altro requisito era di mantenere il servizio in un account AWS separato, per permettere ad un gruppo ristretto di utenti la gestione di Amazon Connect ed altri servizi.

Amazon Connect permette l'utilizzo di AWS Managed Microsoft AD ma, per realizzare la soluzione, abbiamo sfruttato gli Identity Provider aziendali già configurati.

La nostra scelta è ricaduta quindi su AWS SSO. Oltre ad essere molto flessibile nella configurazione di applicazioni SAML, offre la possibilità di implementare il single-sign-on sugli account AWS.

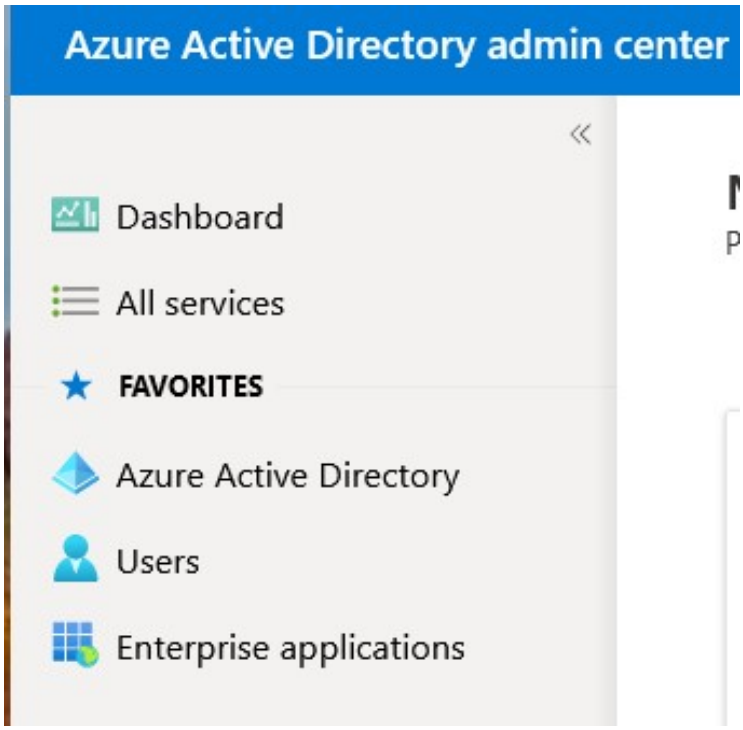
Come vedremo in questo articolo, Amazon Connect non consente di implementare direttamente l'integrazione nativa con AWS SSO. Dovremo quindi configurare un'applicazione SAML ed usarla come identity provider nell'account di destinazione.

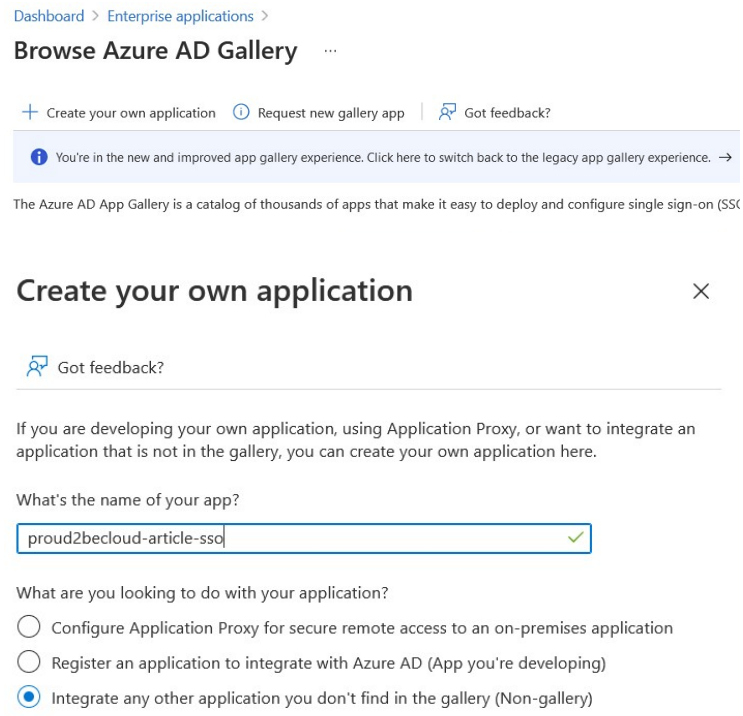
In questo articolo ci occuperemo di:

- Configurare AWS SSO nell'account master dell'organizzazione per utilizzare Azure Active Directory (usato da Office365) ed autenticare gli utenti
- Attivare una istanza Amazon Connect con autenticazione SAML in un account differente nella stessa organizzazione (chiamato internal-services)
- Creare e configurare un'applicazione SAML per Amazon Connect
- Configurare un identity provider nell'account internal-services per autorizzare l'applicazione SAML ed occuparsi dell'autenticazione cross-account
- Aggiungere i ruoli richiesti all'account internal-services per autenticare gli utenti federati
- Collaudare la configurazione

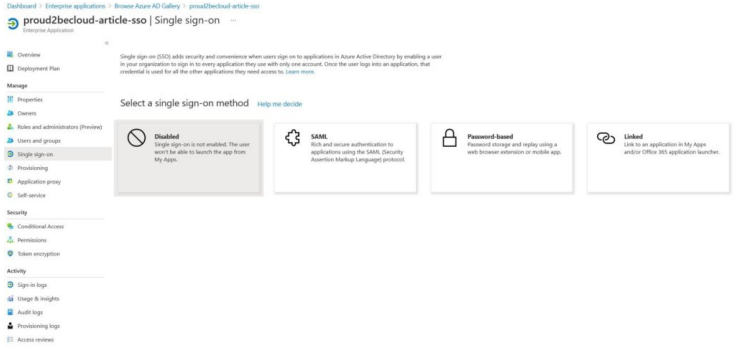
Configurazione di AWS SSO

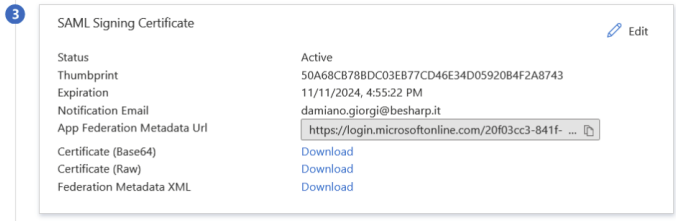
Per prima cosa occorre effettuare il login all'admin center di Azure Active Directory e selezionare "Enterprise Applications". Fare click su "Create your own application" e assegnare un nome univoco





In breve tempo l'applicazione sarà disponibile. A quel punto sarà necessario impostare il **Single sign-on**: fare click sul menu e selezionare "**SAML**"



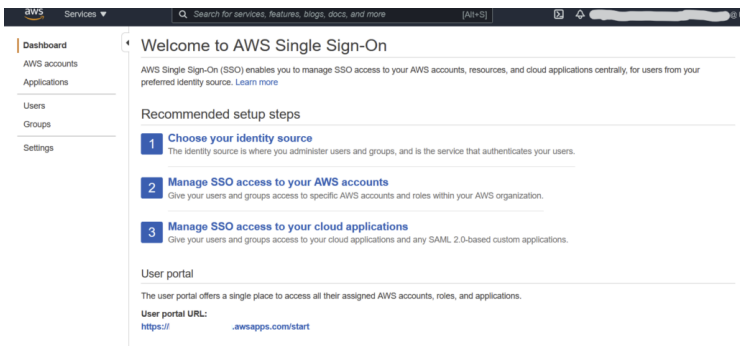


Fare click sul link “**Federation data XML”** e scaricare il file.

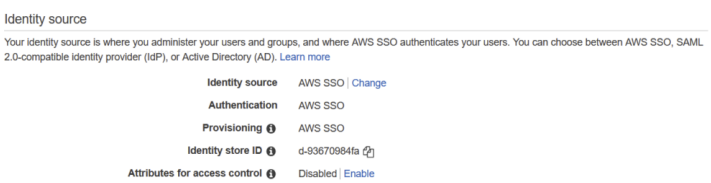
N.B.: il file non dovrà essere condiviso e andrà mantenuto al sicuro.

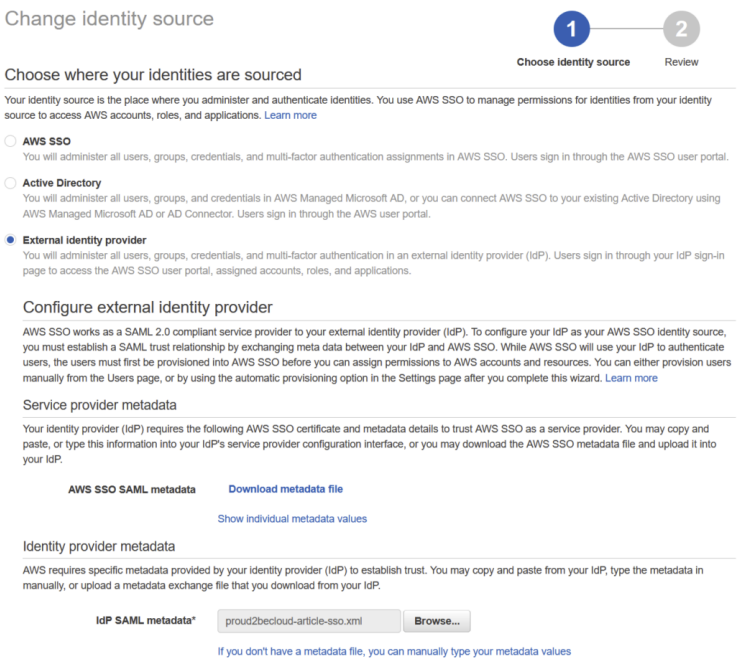
A questo punto è possibile assegnare gli utenti all’applicazione.

Terminata la configurazione dell’applicazione fare login sulla console AWS nell’account di management e selezionare il servizio “**Aws Single Sign on**”



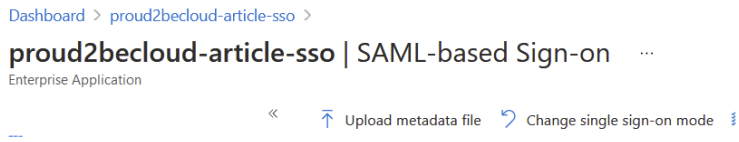
Se AWS SSO è già stato configurato, è sempre possibile cambiare l’identity provider in uso sulla pagina “Settings”





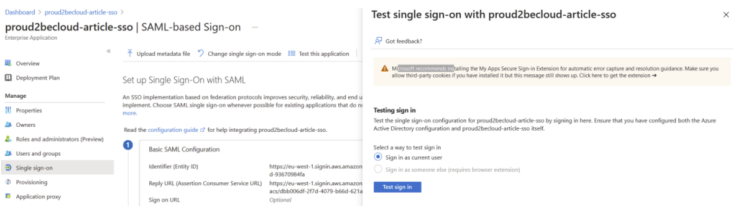
Selezionare “**External identity provider”,** scaricare il metadata file e, come fatto in precedenza, conservarlo in un luogo sicuro.

A questo punto occorre fare upload del file di metadati scaricato dalla console Azure. Sulla console Azure Active Directory Administration fare click su “**upload metadata file”** utilizzando il file scaricato dalla console AWS

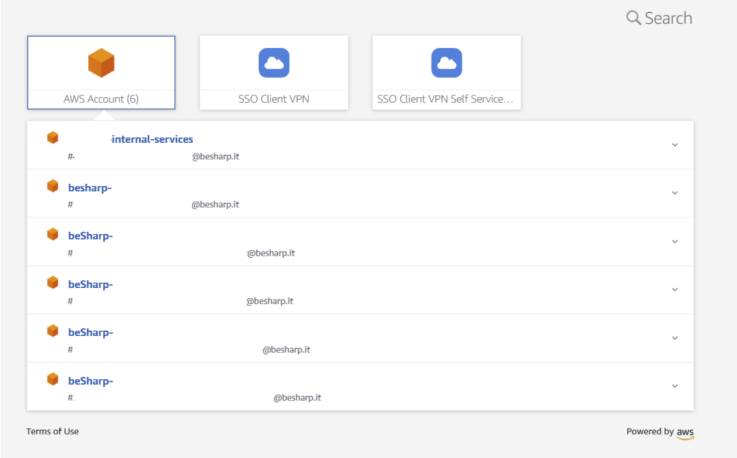


In questo modo, la configurazione della federazione fra Azure Active Directory e AWS SSO è stata portata a termine.

Sulla console Azure è possibile provare l’applicazione, simulando un login con le credenziali correnti.



Se sulla console AWS sono state già assegnate alcune applicazioni sarà possibile vederle ed utilizzarle.

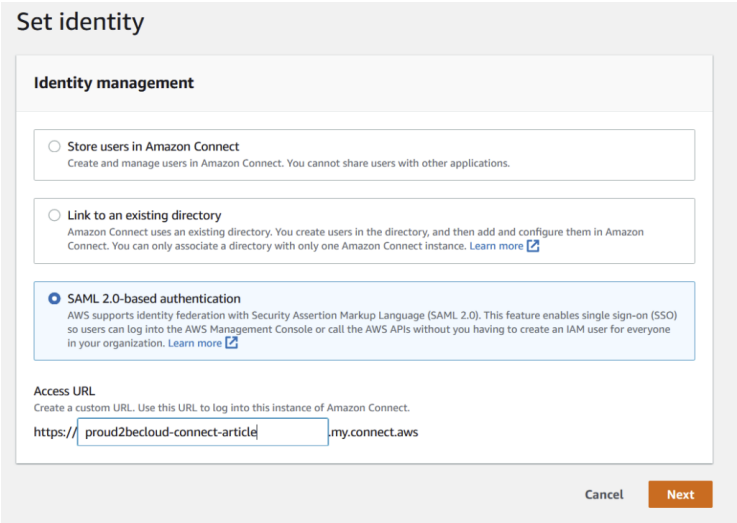


È possibile anche abilitare l'auto provisioning degli utenti ed assegnare gli utenti in modo che siano automaticamente importati su AWS SSO.

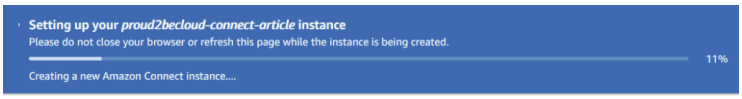
Setup di Amazon Connect

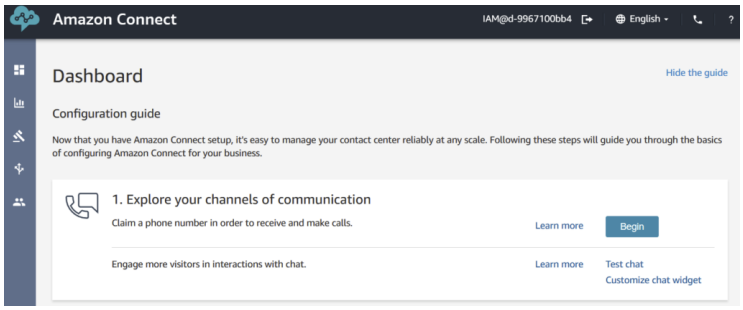
Utilizzeremo un account AWS differente (**internal-services**) per configurare Amazon Connect. Utilizzando AWS SSO e Organization saremo in grado di assegnare permessi molto granulari a differenti utenti e ruoli.

Sull'account internal-service alla sezione "Amazon Connect", fare click su "Create new instance".
Alla sezione "identity management", selezionare "**SAML 2.0-based authentication**".
Una volta selezionato il tipo di autenticazione non sarà più possibile modificarlo.



A questo punto, nel wizard di configurazione, è possibile selezionare le opzioni preferite e procedere con la creazione. Il servizio dopo pochi minuti sarà pronto:

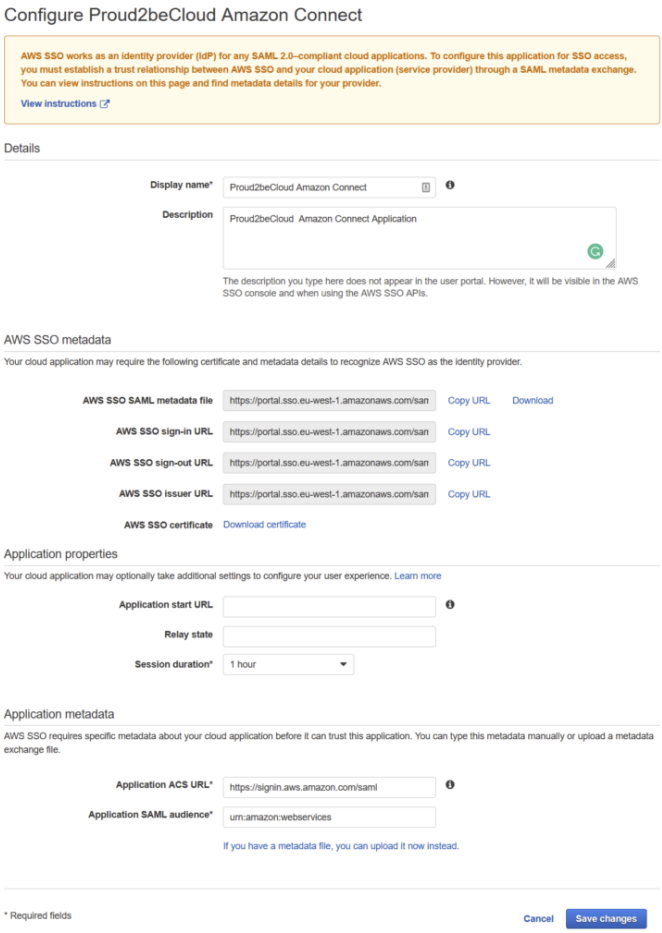




Attenzione: Amazon Connect non supporta il provisioning automatico degli utenti: è necessario creare un utente con lo stesso username definito in Azure Active Directory

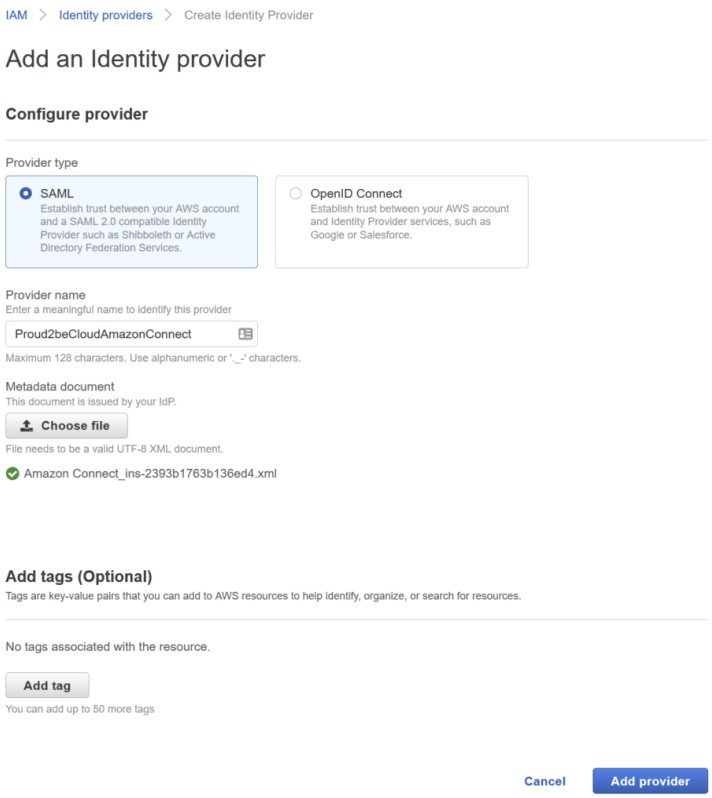
Integrazione Con SSO

Sulla console SSO dell'account di management fare click su "Applications" "Add a new Application", ricercando l'applicazione "**Amazon Connect**".



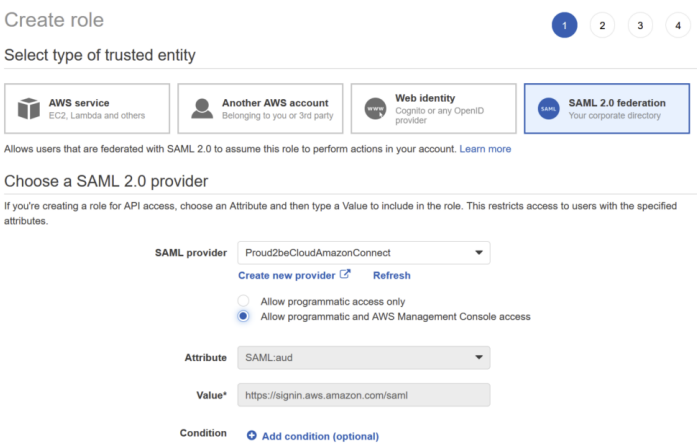
Dopo aver assegnato un nome all'applicazione, fare click su "Download" alla sezione "AWS SSO SAML metadata file".

Nell'account **internal-services** selezionare il servizio IAM e, alla sezione "**Identity Providers"**, fare click su "Add provider" e fare l'upload del metadata file appena caricato



Impostazione dei ruoli

Una volta creato l'identity provider è necessario creare i ruoli e le policy per fare in modo che gli utenti SSO riescano ad accedere al servizio.Nella console IAM dell'account internal-services fare click su Roles e "Create a new Role". Selezionare "**SAML 2.0 federation**" come tipo di trusted identity e selezionare l'identity provider appena creato.

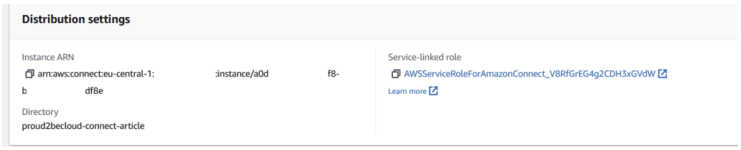


Creare una nuova policy per permettere al ruolo di ottenere un "Federation Token" dall'istanza Amazon Connect, utilizzando questo template json:

```
{
        "Version": "2012-10-17",
        "Statement": [
        {
```

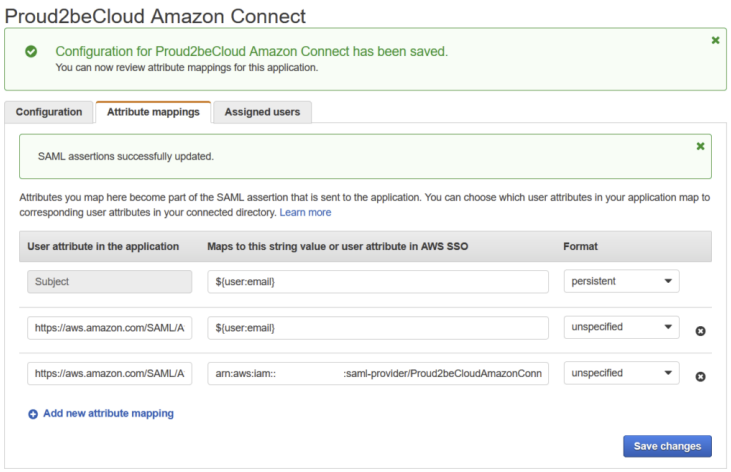
```
                "Sid": "Statement1",
                "Effect": "Allow",
                "Action": "connect:GetFederationToken",
                "Resource": [
                "arn:aws:connect:region:Account-id:instance/amazoncon
nectintanceid/user/${aws:userid}"
                ]
        }
        ]
}
```

È possibile trovare il valore di “amazonconnectinstanceid” facendo click sull’istanza Connect e copiando l’ultima parte del campo “ARN” per **region**:**Account-id** utilizzare invece la region e l’id dell’account internal-service.



Terminata la creazione occorre tornare sulla console AWS SSO sull’account di management e modificare l’applicazione Connect per concludere la configurazione. Selezionare “Edit configuration” e lasciare vuoto il campo “**Application start URL**”. Per il campo “**Relay state”** utilizzare: https://**region**.console.aws.amazon.com/connect/federate/**amazonconnectid** inserendo i valori utilizzati in precedenza.

A questo punto alla sezione "**Attribute Mappings**" aggiungere un nuovo mapping, impostando https://aws.amazon.com/SAML/Attributes/Role come valore per il campo **User attribute in the application**" e arn:aws:iam::**internal-services-account-id**:saml-provider/**saml-provider-name**,arn:aws:iam::**internal-services-account-id**:role/**amazon-connect-federation-role** come valore per il campo "Maps to this string value or user attribute in AWS SSO"



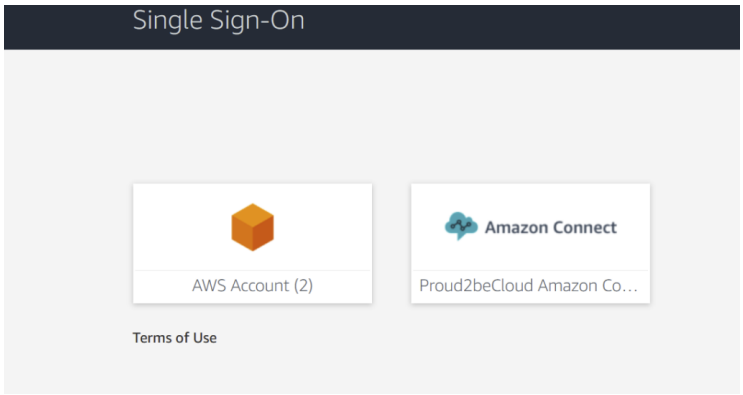
Una volta salvati i cambiamenti assegnare gli utenti utilizzando il tab "**Assigned users**".

Testing

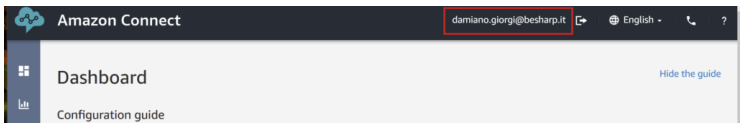
Utilizzare lo "start url" definito in amazon sso (solitamente https://nomeimpostato.awsapps.com/start/) e fare login con le credenziali Azure

AD/Office365.

A questo punto l'applicazione Amazon Connect sarà disponibile.



Facendo click sull'applicazione sarà possibile utilizzare la dashboard di Amazon Connect con le credenziali corrette:



Damiano Giorgi

Ex sistemista on-prem, pigro e incline all'automazione di task noiosi. Alla ricerca costante di novità tecnologiche e quindi passato al cloud per trovare nuovi stimoli.L'unico hardware a cui mi dedico ora è quello del mio basso; se non mi trovate in ufficio o in sala prove provate al pub o in qualche aeroporto!
