Vpn Dialup managed con autenticazione via SSO

8 Giugno 2021 - 6 min. read

AWS Client VPN *AWS Single Sign-On* *Dialup VPN* *Single-Sign-On (SSO)*

In un momento in cui smart working e lavoro da remoto sono entrati nella vita di molti, riuscire a fornire accesso alle risorse aziendali private è un problema all'ordine del giorno.

Una VPN dial-up permette di fornire ad utenti remoti accesso a risorse e servizi non direttamente raggiungibili da internet, anche se tali risorse sono ospitate sul cloud di AWS.

Implementare una soluzione VPN non è mai un compito semplice, specialmente perché alcuni requisiti possono sembrare in contraddizione, come ad esempio:

- Semplicità di configurazione di client e server
- Sicurezza
- Gestione centralizzata

AWS offre il servizio **AWS Client VPN** per facilitare l'accesso remoto alle risorse in VPC, permettendo l'utilizzo di meccanismi di autenticazione esterni come OKTA, Active Directory ed altri servizi che utilizzano il protocollo di autenticazione SAML.

Gli utenti di AWS Client VPN possono utilizzare un portale self-service e scaricare il software e la configurazione, liberando da questi task l'amministratore di sistema.

Scenario di esempio

Qualche tempo fa abbiamo scritto un articolo su come implementare il single-sign-on sulla console AWS utilizzando G Suite per l'autenticazione

In base alle considerazioni fatte vorremmo implementare l'autenticazione usando G Suite come Identity Provider (IdP). Nel fare ciò, abbiamo incontrato una limitazione tecnica su cui stiamo ancora investigando.

La limitazione è data dal fatto che il client software utilizza un servizio http (e non https) per autenticare le richieste, mentre la configurazione dell'autenticazione G Suite accetta solo chiamate https (vedremo più avanti il dettaglio tecnico).

Implementeremo per ora AWS SSO per la parte di autenticazione, in modo da essere in grado in futuro di cambiare il database degli utenti e configurare G Suite come provider.

AWS SSO è utile anche nel caso si utilizzi AWS Organizations per gestire uno scenario multi-account per fornire accessi differenti a diversi account. Alcuni esempi sono disponibili qui.

Utilizzeremo la configurazione di default di SSO con database utenti interni. Le istruzioni di configurazione base sono disponibili qui

Nel nostro esempio daremo accesso agli utenti alle risorse contenute in una VPC in un account di sviluppo.

Nome VPC: test-vpc

CIDR VPC: 172.31.0.0/16

CIDR Client VPN: 172.20.20.0/22 (non deve essere in conflitto con la rete della VPC, né con altre reti che devono essere raggiunte utilizzando la connessione VPN

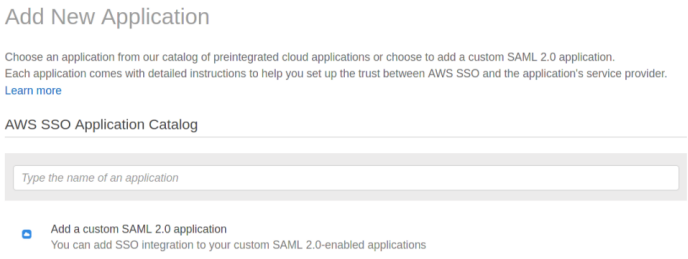
I passi necessari all'implementazione del servizio sono:

- Definire le applicazioni SAML per il portale self-service e l'autenticazione VPN
- Definire gli Identity Provider per il portale self-service e il client VPN
- Creare un Endpoint VPN Client
- Associare le subnet, configurare l'autorizzazione e abilitare il traffico utilizzando i Security Group

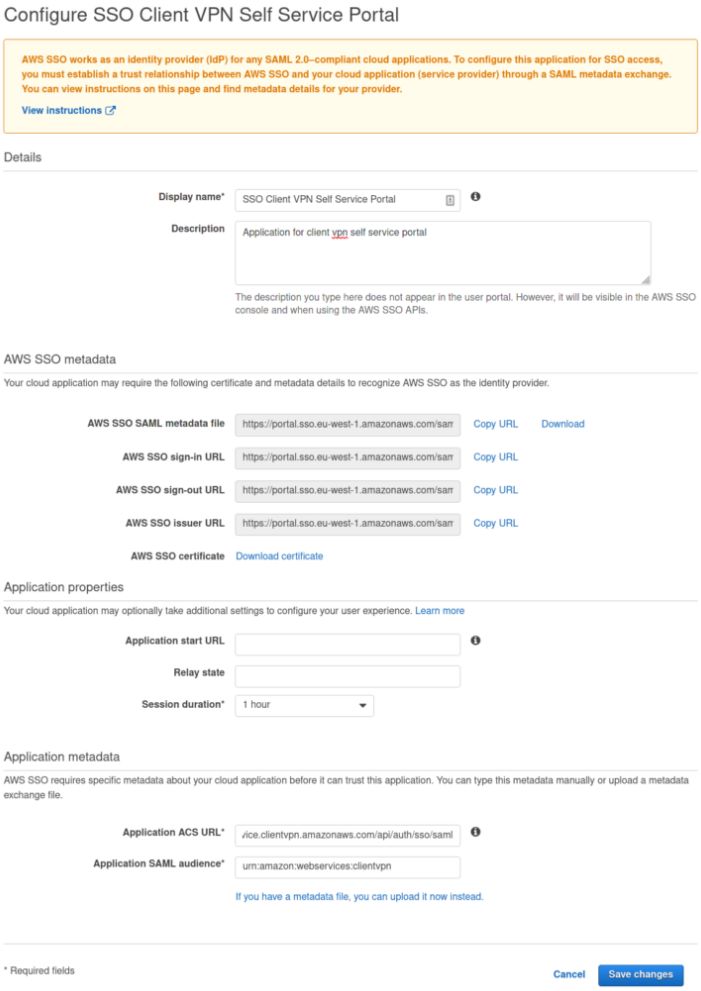
- Test della configurazione

Definire le applicazioni SAML

Per permettere al client VPN di autenticare gli utenti dobbiamo definire due applicazioni SAML: una per il portale self-service ed una per l'applicazione desktop client.
Nell'account master dell'organizatione selezionare "**AWS Single Sign-On**", "**Applications**", "**Add a new application**", "**Add a custom SAML 2.0 Application**"



A questa applicazione daremo il nome "SSO Client VPN Self Service Portal"



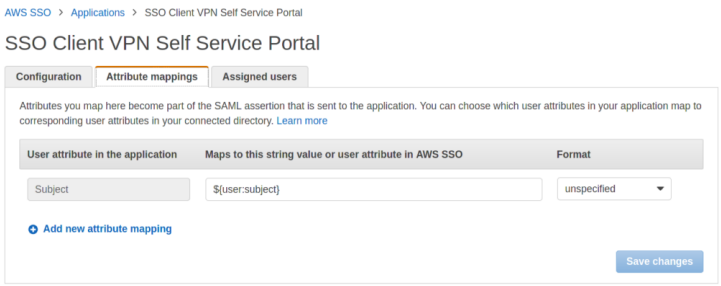
A questo punto fare click sul link "**Download**" in fianco alla voce "AWS SSO SAML metadata file". Il file contiene informazioni sensibili, per cui **va mantenuto segreto**.

Alla sezione “Application Metadata” selezionare "**Manually type your metadata values**” ed inserire le informazioni:

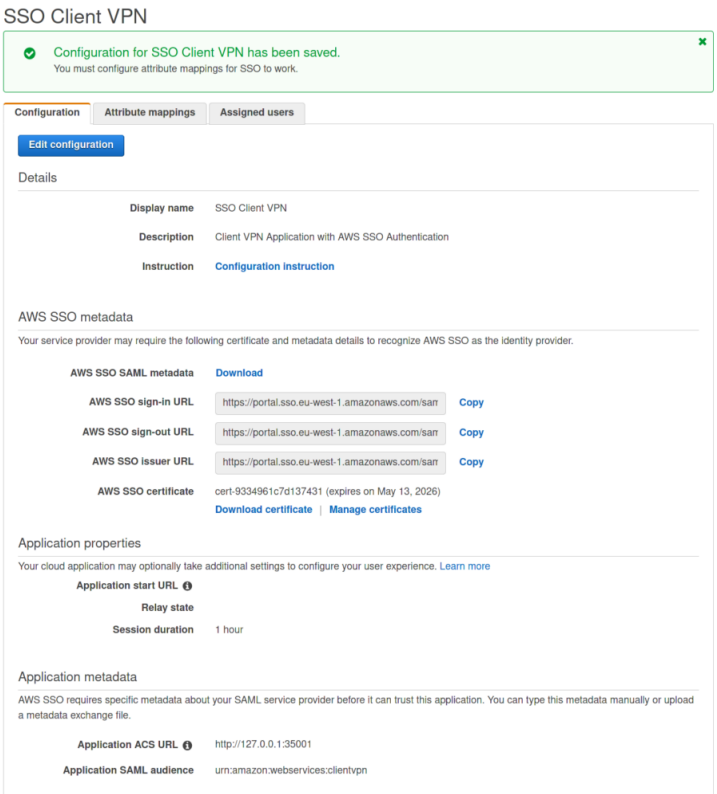
Application ACS URL: https://self-service.clientvpn.amazonaws.com/api/auth/sso/saml
Application SAML Audience: urn:amazon:webservices:clientvpn

Application SAML Audience: urn:amazon:webservices:clientvpn

Selezionare la scheda “Attributes mappings” e inserire il valore ${user:subject} nel campo “Subject”, in questo modo il valore sarà mappato automaticamente.



Dopo aver aggiunto l’applicazione per il portale self-service occorre aggiungere l’applicazione per il client VPN:



Come prima salvare il file metadati e mantenerlo segreto, per la sezione “Application metadata” utilizzare invece i valori:

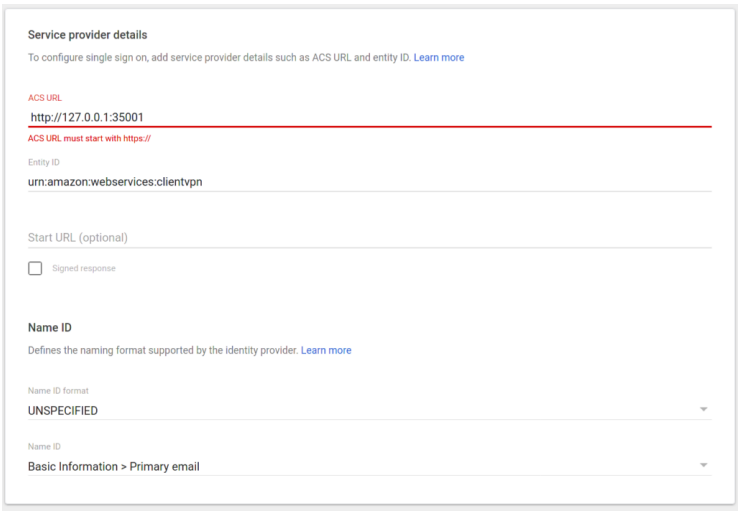
Application ACS URL: http://127.0.0.1:35001

Application SAML Audience: urn:amazon:webservices:clientvpn

Scarichiamo il metadata e**teniamolo segreto.**

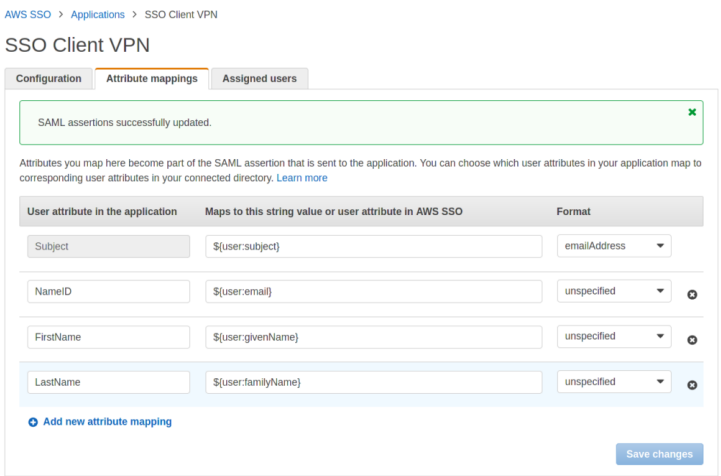
Il campo ACS URL è insolito: http://127.0.0.1.

Questo perché l'applicazione client esegue un servizio sul computer locale per validare e inoltrare i dati di autenticazione SAML. Questo è il motivo per cui l'autenticazione G Suite non è configurabile in modo semplice ed occorre una analisi più approfondita. Provando a configurare l'applicazione SAML in G Suite si ottiene infatti l'errore di validazione:



Spoiler: con un piccolo hack è possibile superare la validazione e forzare il valore. Vedremo nel dettaglio come in un articolo specifico, quindi seguiteci!

Dopo aver aggiunto l'applicazione per il Client VPN selezionare il tab "Attributes mappings" ed inserire i valori come in figura:



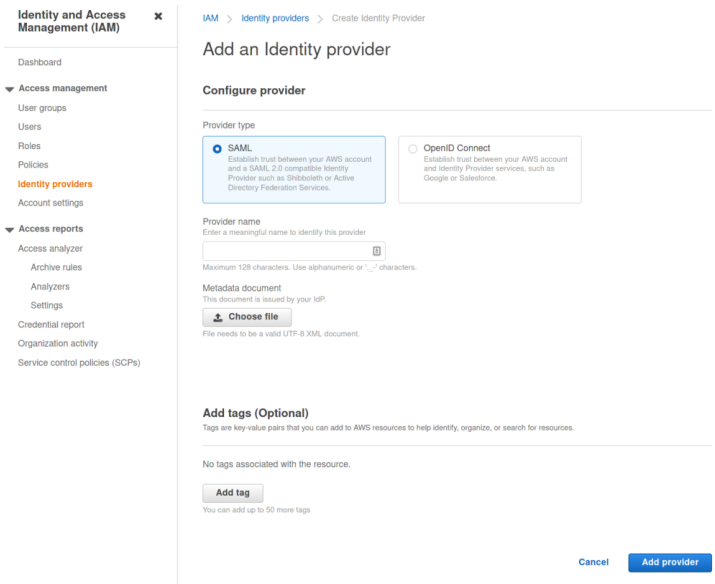
Nel caso i campi non siano configurati correttamente, l'autenticazione fallirà. Prestate attenzione al formato del campo "Subject", occorre cambiare il valore predefinito e sostituirlo con "**emailAddress**".

Dopo aver aggiunto le applicazioni SAML occorre configurare l'account di destinazione (development nel nostro caso) per fare in modo che le applicazioni siano utilizzate

come identity provider. (Non dimenticate di assegnare gli utenti alle applicazioni usando la tab “Assigned users”, altrimenti non saranno disponibili una volta effettuato il login.

Definire gli Identity Provider per il portale self-service e il client VPN

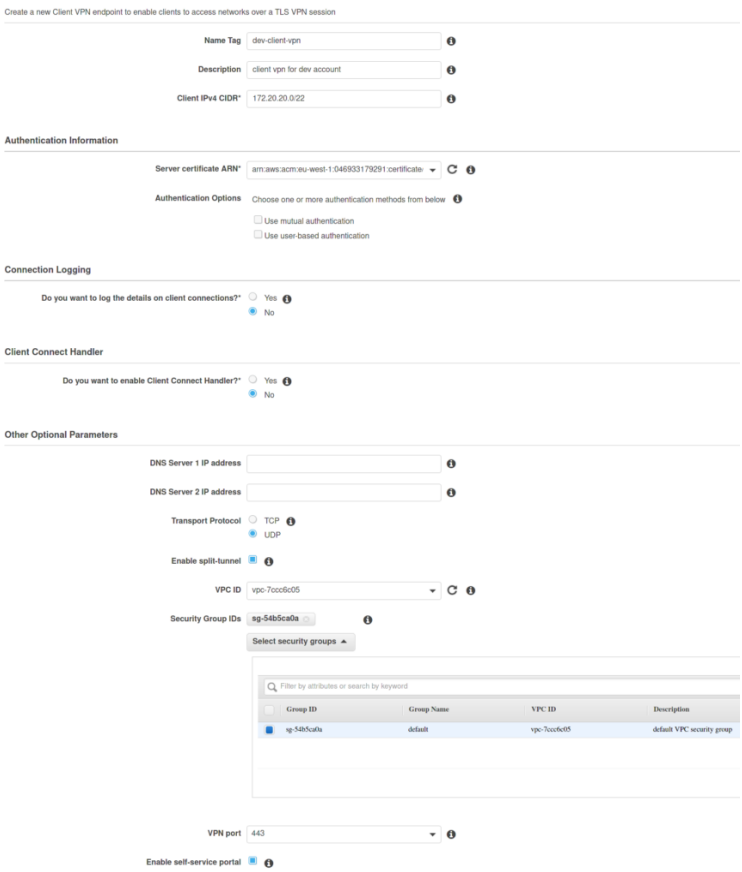
Sulla console dell’account “development” alla sezione "**Identity Providers**” di **IAM** fare click su “**Add provider**”.
Selezionare SAML, inserire un nome (utilizzeremo *clientvpn-sso-idp* per il client VPN e *clientvpn-portal-idp* per il portale self-service) e selezionare i file metadata file scaricati in precedenza. Procediamo con l'upload



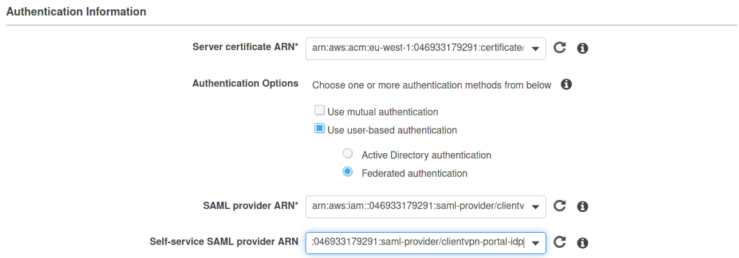
Ora è possibile creare il VPN Client endpoint nella vpc e configurarlo per utilizzare le applicazioni SAML per l’autenticazione.

Creazione del Client VPN Endpoint

Un requisito per la creazione dell’endpoint è la creazione di un certificato ACM associato al dominio. Se un certificato non è disponibile basta crearlo seguendo i passaggi descritti nella documentazione.
Nell’account di development alla sezione “**Client VPN Endpoints**” della VPC selezionare “**Create a new client vpn endpoint**”

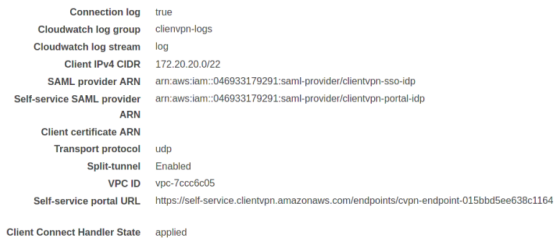


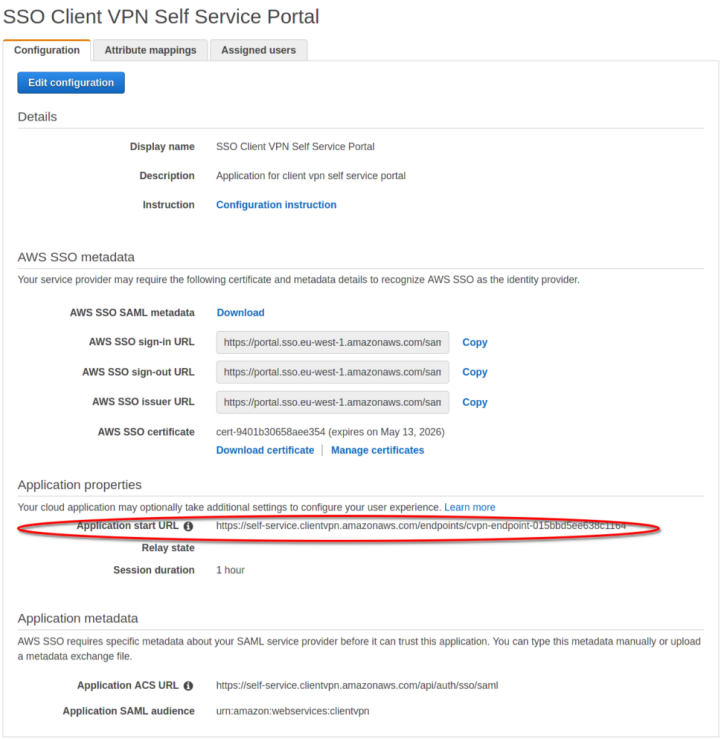
Selezionare “**Use user-based authentication**” e utilizzare i due IdP creati in precedenza:



Non dimenticatevi di selezionare la casella “**Enable self-service portal**”

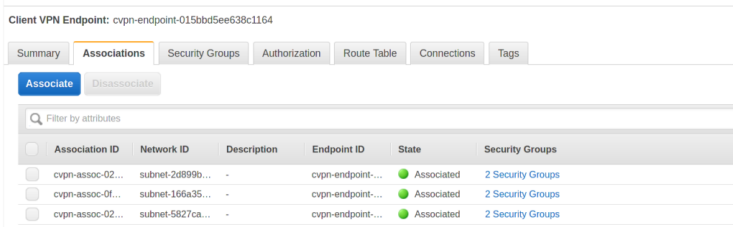
Dopo aver salvato la configurazione, occorre copiare l’URL del self-service portal ed impostarla come “Application start URL” per l’applicazione “SSO Client VPN service portal” che abbiamo definito in precedenza. In questo modo gli utenti saranno indirizzati alla pagina corretta:



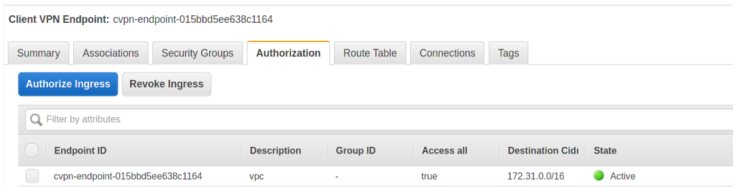


Associare le subnet, configurare l'autorizzazione e abilitare il traffico utilizzando i Security Group

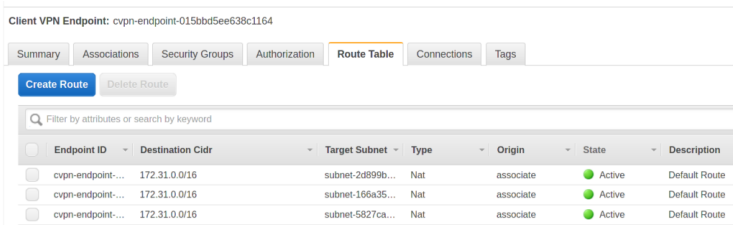
Cliccare sulla tab "Associations" sul Client VPN endpoint, selezionare la VPC di destinazione e la subnet (o le subnet) da associare. Dopo alcuni istanti lo stato cambierà in "associated":



Fare click sul tab "Associations" e autorizzare l'accesso alla rete della VPC:



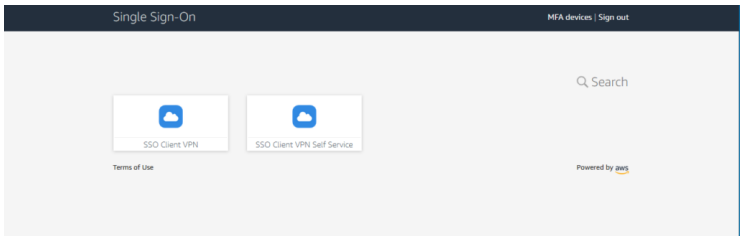
Le regole di routing saranno aggiunte in automatico:



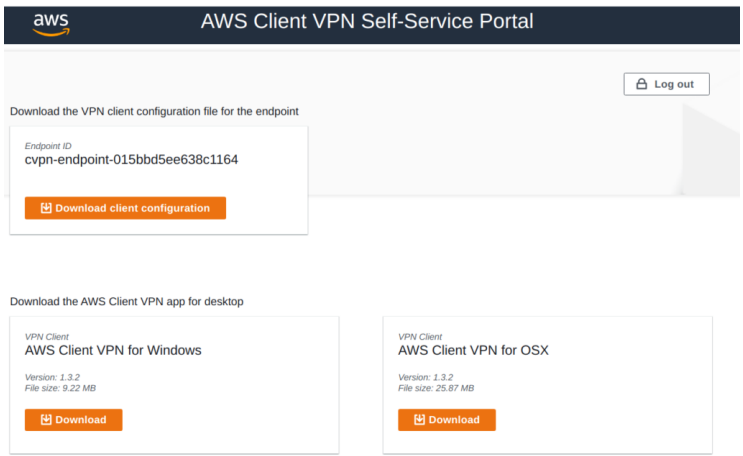
Test della configurazione

In una finestra privata (o in un'altra sessione del browser) immettere l'indirizzo dello user portal SSO (ad esempio: https://example-org.awsapps.com/start)

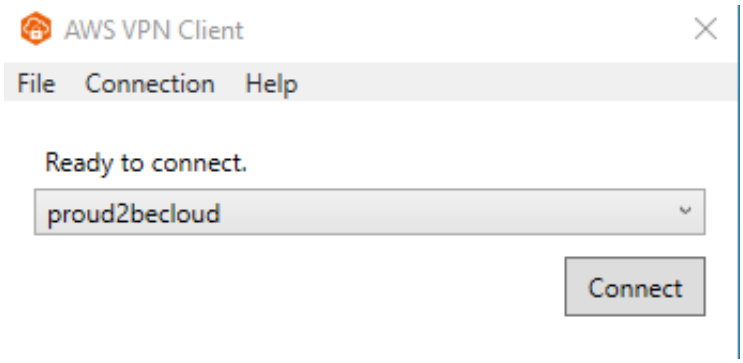
Dopo aver effettuato il login, si vedranno le due applicazioni configurate:



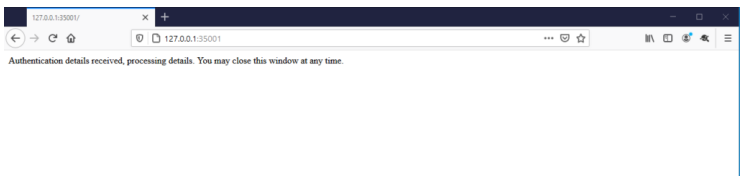
Selezionando l'applicazione "SSO Client VPN Self Service" si verrà reindirizzati al portale che permette di scaricare la configurazione ed il software client.



Dopo aver installato il client, è possibile importare la configurazione (file -> manage profiles - add profile)

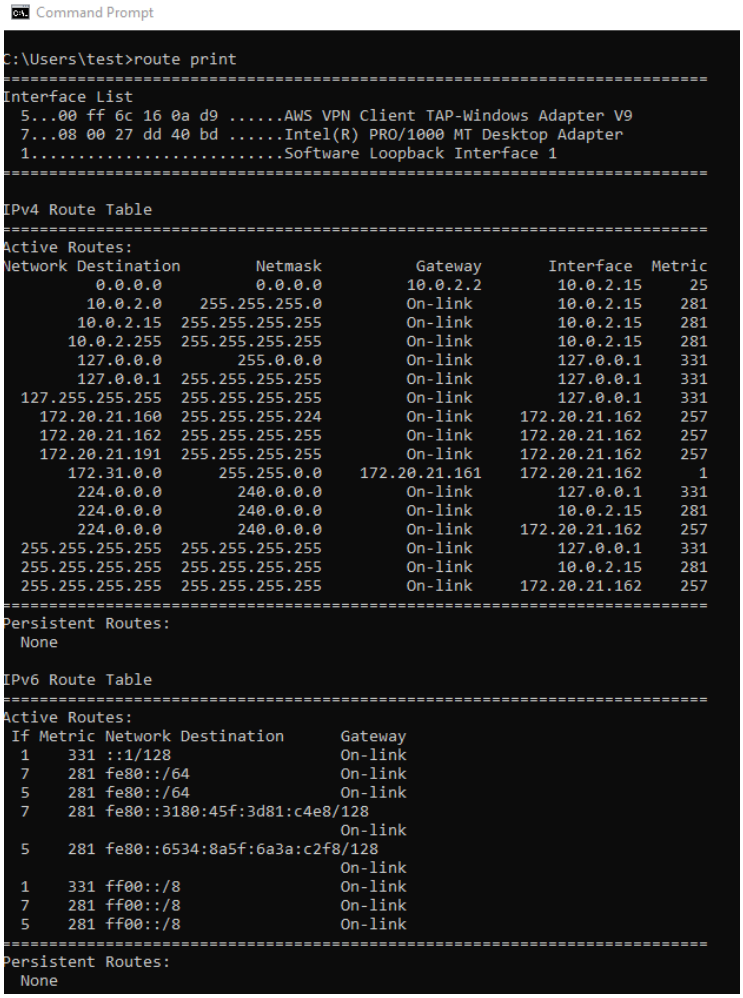


Cliccare su "connect". Si aprirà una nuova finestra del browser con la richiesta delle credenziali di autenticazione. Una volta effettuato il login sarà visualizzato un messaggio di conferma:



Sulla console alla sezione "Client vpn endpoints" usando la tab "Connections" si vedranno le connessioni:

Sul client si vedranno le regole di routing aggiunte automaticamente per raggiungere la VPC:



Conclusioni

Il Client AWS VPN è un servizio managed che facilita la configurazione delle connessioni VPN per gli utenti finali, offre un meccanismo di configurazione semplice e automatizzato. In questo articolo abbiamo esplorato una implementazione personalizzata non descritta nella documentazione ufficiale.

Siamo ancora alla ricerca della modalità migliore per aggiungere G Suite come provider di identità per AWS SSO e utilizzare le applicazioni SAML per impostare gli attributi corretti per l'autenticazione. E voi lo avete già fatto? Ci vediamo tra 14 giorni su **#Proud2beCloud** con un nuovo articolo!

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!

Simone Merlini

CEO e co-fondatore di beSharp, Cloud Ninja ed early adopter di qualsiasi tipo di soluzione *aaS. Mi divido tra la tastiera del PC e quella a tasti bianchi e neri; sono specializzato nel deploy di cene pantagrueliche e nel test di bottiglie d'annata.
