

Home > Networking & Content Delivery

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"

Add	New Application
Choose Each aj <mark>Learn n</mark>	e an application from our catalog of preintegrated cloud applications or choose to add a custom SAML 2.0 application. pplication comes with detailed instructions to help you set up the trust between AWS SSO and the application's service provider. nore
AWS	SSO Application Catalog
Тур	e the name of an application
0	Add a custom SAML 2.0 application You can add SSO integration to your custom SAML 2.0-enabled applications

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

View instructions C		
Details		
Display name*	SSO Client VPN Self Service Portal	θ
Description	Application for client ypn self service portal	
	The description you type here does not appear in the console and when using the AWS SSO APIs.	user portal. However, it will be visible in the AWS
AWS SSO metadata		
Your cloud application may require the following certil	licate and metadata details to recognize AWS SSO as	the identity provider.
AWS SSO SAML metadata file	https://portal.sso.eu-west-1.amazonaws.com/sam	Copy URL Download
AWS SSO sign-in URL	https://portal.sso.eu-west-1.amazonaws.com/sam	Copy URL
AWS SSO sign-out URL	https://portal.sso.eu-west-1.amazonaws.com/sam	Copy URL
AWS SSO issuer URL	https://portal.sso.eu-west-1.amazonaws.com/sam	Copy URL
AWS SSO certificate	Download certificate	
Application properties Your cloud application may optionally take additional	settings to configure your user experience. Learn more	
Application start URL		0
Relay state		
Session duration*	1 hour 💌	
Application metadata		
AWS SSO requires specific metadata about your clou exchange file.	d application before it can trust this application. You ca	an type this metadata manually or upload a metad
Application ACS URL*	vice.clientvpn.amazonaws.com/api/auth/sso/saml	0
Application SAML audience*	um:amazon:webservices:clientvpn	
	If you have a metadata file, you can upload it now ins	tead.

Configure 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:

 Config You mus 	uration for SSO Clier t configure attribute mappi	nt VPN has been saved. ngs for SSO to work.	
Configuration	Attribute mappings	Assigned users	
Edit configura	ation		
Details			
	Display name	SSO Client VPN	
	Description	Client VPN Application with AWS SSO Authentical	ion
	Instruction	Configuration instruction	
AWS SSO m	etadata	the contract and exclude to the lower of the All	
Your service pro	vider may require the tollow	ving certificate and metadata details to recognize Av	IS SSO as the identity provider.
AWS	SSO SAML metadata	Download	
	AWS SSO sign-in URL	https://portal.sso.eu-west-1.amazonaws.com/sal	г Сору
A	WS SSO sign-out URL	https://portal.sso.eu-west-1.amazonaws.com/sar	г Сору
	AWS SSO issuer URL	https://portal.sso.eu-west-1.amazonaws.com/sal	г Сору
	AWS SSO certificate	cert-9334961c7d137431 (expires on May 13, 2026	;)
		Download certificate Manage certificates	
Application p	roperties		
Your cloud applic	cation may optionally take	additional settings to configure your user experience	Learn more
Ap	plication start URL 🚯		
	Relay state		
	Session duration	1 hour	
Application m	netadata		
AWS SSO requir a metadata exch	es specific metadata abou ange file.	t your SAML service provider before it can trust this	application. You can type this metadata manually or uploa
Ap	plication ACS URL 🚯	http://127.0.0.1:35001	

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 eteniamolo 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:

Service provider d	etails
To configure single s	gn on, add service provider details such as ACS URL and entity ID. Learn more
ACSURE	
http://127.0.0.1:3	5001
ACS URL must start with	https://
Entity ID	
urn:amazon:webse	ervices:clientvpn
Start URL (optiona	0
Signed response	
Name ID	
Defines the naming f	ormat supported by the identity provider. Learn more
Name ID format	
Name ID format	
Name ID format	v

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:

	Attribute mappings	Assigned users	
SAML asser	tions successfully updated	L.	
ttributes you m prresponding u	ap here become part of th ser attributes in your conn	e SAML assertion that is sent to the application. You can c ected directory. Learn more	hoose which user attributes in your application ma
Cubicet	in the application	(usersublest)	
Subject		\${user.subject}	emainAddress
NameID		\${user:email}	unspecified -
EirstName		\${user:givenName}	unspecified -
Filoavanie			

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

Identity and Access 🛛 🗙 Management (IAM)	IAM > Identity providers > Create Identity Provider
Dashboard	Add an Identity provider
Access management	Configure provider
User groups	
Users	Provider type
Roles	O SAML OpenID Connect
Policies	Establish trust between your AWS account and a SAML 2.0 compatible identity and identity Provider services, such as
Identity providers	Provider such as Shibboleth or Active Google or Salesforce. Directory Federation Services.
Account settings	
Access reports	Provider name
Access analyzer	
Archive rules	Maximum 128 characters. Use alphanumeric or ',' characters.
Analyzers	Metadata document
Settings	This document is issued by your IdP.
Credential report	± Choose file
Organization activity	File needs to be a valid UTF-8 XML document.
Service control policies (SCPs)	
	Add tags (Optional) Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources. No tags associated with the resource. Add tag You can add up to 50 more tags

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**"

create a new crient view endpoint to enable clients to access networks	a over a TLS VPN session			
Name Tag	dev-client-vpn	0		
Description	client vpn for dev account	0		
Client IPv4 CIDR*	172.20.20.0/22	0		
Authentication Information				
Server certificate ARN*	arn:aws:acm:eu-wesi-1:046933179291:certificate/ 👻	CO		
Authentication Options	Choose one or more authentication methods from below	0		
	Use mutual authentication			
	Use user-based authentication			
Connection Logging				
Do you want to log the details on client connections?*	 Yes () ● No 			
Client Connect Handler				
Do you want to enable Client Connect Handler?*	Yes 🚯			
	No			
Other Optional Parameters				
DNS Server 1 IP address		0		
DNS Server 2 IP address		0		
Transport Protocol	О ТСР ()			
Enable split-tunnel				
Enable split-tunnel	• • • • • • • • • • • • • • • • • • •	C 0		
Enable split-tunnel VPC ID Security Group IDs	vpc-7ccc6c05 v	C 0		
Enable spill-lunnel VPC ID Security Group IDs	vpc 7ccc8c05 sg-54b5ca0a	CO		
Enable split-kunnel VPC ID Security Group IDs	O vpc7coc6c05 vpc sp-54b5cn0a O Select security groups *	C O		
Enable split-kunnel VPC ID Security Group IDs		Ce	VPC ID	Devolution
Enable split-kunnel VPC ID Security Group IDa		C 0	VPC ID vpc-7ccefed5	Description default VPC security grou
Enable split-kunnel VPC ID Security Group IDs	O vpo 7 bocoldol so, 54b5cath O Select security groups C Group ID Group ID Group ID Group Ma g. 54bcath delat	С 9 «	VPC ID spc-7code05	Description default VFC security grow
Enable split-kunnel VPC ID Security Group IDs	pop-focceledds sp-54b5carba O Select security groups Comp Da Group DB Group NB g-54b5carba data	С 0 «	VPC ID spc-Teoded5	Description default VPC security grow
Enable split-kunnel VPC ID Security Group IDs	pop-focceledds sp-5485carba O Select security groups Comp Data g-10hr by an blutte or search by keyword Group DB Group XB g-5485carba ddata	C 0	VPC ID ypc-7code05	Description default VPC security grou

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:

Connection log	true
Cloudwatch log group	clienvpn-logs
Cloudwatch log stream	log
Client IPv4 CIDR	172.20.20.0/22
SAML provider ARN	arn:aws:iam::046933179291:saml-provider/clientvpn-sso-idp
Self-service SAML provider	arn:aws:iam::046933179291:saml-provider/clientvpn-portal-idp
ARN	
Client certificate ARN	
Transport protocol	udp
Split-tunnel	Enabled
VPC ID	vpc-7ccc6c05
Self-service portal URL	https://self-service.clientvpn.amazonaws.com/endpoints/cvpn-endpoint-015bbd5ee638c1164
Client Connect Handler State	applied

SSO Client VPN Self Service Portal

Configuration Att	ribute mappings	Assigned users	
Edit configuration			
Luk configuration			
Details			
	Display name	SSO Client VPN Self Service Portal	
	Description	Application for client vpn self service portal	
	Instruction	Configuration instruction	
AWS SSO metada	ata		
'our service provider n	nay require the follow	ving certificate and metadata details to recogniz	e AWS SSO as the identity provider.
AWS SSO	SAML metadata	Download	
AWS S	SSO sign-in URL	https://portal.sso.eu-west-1.amazonaws.com	n/san Copy
AWS SS	60 sign-out URL	https://portal.sso.eu-west-1.amazonaws.com	n/san Copy
AWS	SSO issuer URL	https://portal.sso.eu-west-1.amazonaws.com	n/san Copy
AWS	SSO certificate	cert-9401b30658aee354 (expires on May 13,	2026)
		Download certificate Manage certificate	S
Application prope	rties		
our cloud application	may optionally take	additional settings to configure your user experie	ence. Learn more
Applicati	on start URL 🚯	https://self-service.clientvpn.amazonaws.com/	endpoints/cvpn-endpoint-015bbd5ee638c1164
	Relay state		
S	ession duration	1 hour	
Application metad	lata		
WS SSO requires spe metadata exchange f	ecific metadata abou file.	t your SAML service provider before it can trust	this application. You can type this metadata manually or uplo
Applicati	ion ACS URL 🚯	https://self-service.clientvpn.amazonaws.com/	'api/auth/sso/saml
Application	SAML audience	urn:amazon:webservices:clientvpn	

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":

ent VPN Endpoint: cvp	n-endpoint-015bbd5e	e638c1164					
Summary Association	ons Security Gro	ups Authoriza	tion Route Table	e Connections	Tags		
Associate Disasso							
Q. Filter by attributes							
C Filter by attributes							
Association ID	Network ID	Description	Endpoint ID	State	Security Groups		
Association ID cvpn-assoc-02	Network ID subnet-2d899b	Description	Endpoint ID cvpn-endpoint	State Associated	Security Groups 2 Security Groups		
Association ID cvpn-assoc-02 cvpn-assoc-0f	Network ID subnet-2d899b subnet-166a35	Description	Endpoint ID cvpn-endpoint cvpn-endpoint	State Contemporate State	Security Groups 2 Security Groups 2 Security Groups		

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

Client VPN E	ndpoint: cvpn-end	dpoint-015bbd5ee638	3c1164					
Summary	Associations	Security Groups	Authorization	Route Table	Connections	Tags		
Authorize	e Ingress Revo	oke Ingress						
Q, Filter	by attributes							
End	lpoint ID		Description	Group ID	Access all	Destination Cidi	State	
сур	n-endpoint-015bbd5	ee638c1164	vpc		true	172.31.0.0/16	Active	

Le regole di routing saranno aggiunte in automatico:

Slient VPN Endpoint: cvpn-endpoint-015bbd5ee638c1164										
Summary	Associations	s Security Groups	Authorization	Route Table	Connections	Tags				
Create R	oute Delete									
Q, Filter	by attributes or s	search by keyword								
En	dpoint ID 🛛 👻	Destination Cidr	Ŧ	Target Subnet 👻	Туре	Origin	÷	State	~	Description
cvp	n-endpoint	172.31.0.0/16		subnet-2d899b	Nat	associate		Active		Default Route
cvp	n-endpoint	172.31.0.0/16		subnet-166a35	Nat	associate		Active		Default Route
cvp	n-endpoint	172.31.0.0/16		subnet-5827ca	Nat	associate		Active		Default Route

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.

aws AWS Client VPN Self-Service Portal					
Download the VPN client configuration file for the endpoint		A Log out			
Endpoint ID cvpn-endpoint-015bbd5ee638c1164					
Download client configuration					
VPV/Client AWS Client VPN for Windows Version: 1.3.2 File size: 9.22 MB	VPN Client AWS Client VPN for OSX Version: 1.3.2 File size: 52.7 MB				

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:

127.0.0.1:35001/	× +		
← → ♂ ☆	0 127.0.0.1:35001	… ☺ ☆	li\ ⊡ \$* 4< ≡
Authentication details received, p	processing details. You may close this window at any time.		

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:

command Prompt							
C:\Users\test>route print							
Interface List							
500 ff 6c 16	0a d9AWS V	'PN Client TAP-Wind	ows Adapter V9				
708 00 27 dd	40 bdIntel	(R) PRO/1000 MT De	sktop Adapter				
1	Softw	are Loopback Inter	face 1				
Thus have to bla							
IPV4 Route Table							
Activo Poutos:			================				
Network Destinatio	n Netmask	Gateway	Intenface	Matric			
	0 0 0 0	10 0 2 2	10 0 2 15	25			
10 0 2 0	255 255 255 0	On-link	10.0.2.15	281			
10 0 2 15	255 255 255 255	On-link	10.0.2.15	281			
10 0 2 255	255 255 255 255	On-link	10.0.2.15	281			
127.0.0.0	255.0.0.0	On-link	127.0.0.1	331			
127.0.0.1	255.255.255.255	On-link	127.0.0.1	331			
127.255.255.255	255.255.255.255	On-link	127.0.0.1	331			
172.20.21.160	255.255.255.224	On-link	172.20.21.162	257			
172.20.21.162	255.255.255.255	On-link	172.20.21.162	257			
172.20.21.191	255.255.255.255	On-link	172.20.21.162	257			
172.31.0.0	255.255.0.0	172.20.21.161	172.20.21.162	1			
224.0.0.0	240.0.0.0	On-link	127.0.0.1	331			
224.0.0.0	240.0.0.0	On-link	10.0.2.15	281			
224.0.0.0	240.0.0.0	On-link	172.20.21.162	257			
255.255.255.255	255.255.255.255	On-link	127.0.0.1	331			
255.255.255.255	255.255.255.255	On-link	10.0.2.15	281			
255.255.255.255	255.255.255.255	On-link	172.20.21.162	257			
Persistent Routes:							
None							
IPv6 Route Table							
			=================				
ACTIVE ROUTES:	Destination	Catavav					
1 221 ···1/120	bestination	On link					
7 201 50000	64	On link					
5 281 fe80/	64	On-link					
7 281 fe80::7	3180·15f·3d81·c168	2/128					
/ 201 (000	100.451.5001.0400	On-link					
5 281 fe806	5 281 fe80: 6534:8a5f:6a3a:c2f8/128						
0n-link							
1 331 ff00::/	/8	On-link					
7 281 ff00::/	/8	On-link					
5 281 ff00::/	/8	On-link					
Persistent Routes:							
Nono							

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.

Copyright © 2011-2021 by beSharp srl - P.IVA IT02415160189