

Home > Networking & Content Delivery

VPC Lattice: yet another connectivity option or a game-changer?

12 April 2024 - 4 min. read

Advanced Networking

VPC Lattice

"Live as if you were to die tomorrow. Learn as if you were to live forever"

- Mahatma Gandhi

I like learning new things, and I am lucky because a significant part of my work involves learning new technologies and evaluating how to use them to solve new and existing problems.

In the past few years, we described many connectivity options to connect our workloads running on AWS (Transit Gateways, Load balancing, Shared VPCs, PrivateLink and Endpoint Services, and VPC peering...)

Last year, **VPC Lattice** reached General Availability, offering a new option for us to explore. You may be wondering why we should learn how to use another service when we already have so many options to choose from... Well, let's find out!

In this article, we'll see that we needed to add another thing... Let's see what this service offers, how it differs from the other connectivity options we already know, and a simple use case.

So, without any further ado, let's dig in!

Where VPC Lattice stands

As we saw in previous articles, microservices are an architectural approach that allows developers to build and deploy software faster. How Was this article useful for you?

single applications now consist of numerous individ distributed in different AWS accounts and must cor various technologies can be used together: Lambda

We must face tasks like service discovery, traffic rol detailed metrics. There are scenarios where a strict authorization policy is complex to implement using



Think about allowing communication only between two microservices in different AWS accounts, blocking every other traffic without implementing custom solutions and authentication.

VPC Lattice aims to help organizations overcome these challenges while keeping a secure and manageable approach.

It enables developers to manage microservices definition, authorization, and configuration, while administrators can manage infrastructure, network, communication policies, and governance; we'll see more in the following sections.

VPC Lattice Components

VPC Lattice has some key components:

- **Service**: a VPC Lattice service represents an application and its resources: computational (such as lambdas, EKS pods, EC2 instances), listeners (port and protocols involved), and routing rules to address traffic (weighted routing, path routing, and so on). The application team typically manages these aspects and can be autonomously defined. A service can be shared using AWS Resource Access Manager with other AWS accounts, even outside an organization.
- Service Network: a service network is a new concept because it's a logical grouping of services that facilitates connectivity. It can also be shared using AWS Resource Access Manager. This kind of resource is usually defined by infrastructure or network administrators.
- Service Directory: the list of service networks that can be used, shared with AWS RAM
- Auth Policies: IAM documents that can define access to resources. Auth policies differ from IAM policies because they aren't attached to users, groups, or roles but are used with services and service networks. The

or other services access to the attached service. conditions, such as

vpc-lattice-svcs:RequestMethod

Was this article useful for you?

Yes!
I was expecting something different

Made with Hotjar

to filter allowed methods. For a complete list, you o documentation.

Let's see which steps are required to set up VPC Lattice.

Putting all together

Let's briefly look at the roles and steps involved in setting up the communication.

- 1. The infrastructure admin defines a **Service Network**
- 2. The infrastructure admin shares the Service Network using AWS RAM
- 3. The service owner defines a **VPC Lattice Service** and its authorization policies
- 4. The service owner associates the **Service** with the Service Network
- 5. The infrastructure admin **associates** the Service Network with the **VPCs**

As you can see, there is a certain degree of independence in managing services, so dependencies between teams and operations are reduced.

A practical example of VPC Lattice usage

For our example, we will use the sample infrastructure and applications from this URL and analyze the key components deployed on the AWS Console.

You can deploy the reference architecture using the instructions contained in the *ReadMe* file in the repository.

You can also use three different VPCs belonging to a single account to ease the deployment process (as we'll do in this article).

You'll end with this sample infrastructure:



Image source: https://github.com/aws-samples/build-secure-multi-account-vpcconnectivity-applications-with-amazon-vpc-lattice

In our example, App1 and App2 will need to communicate bidirectionally, and App3 will be consumed by App1, App2, and App4.



Image source: https://github.com/aws-samples/build-secure-multi-account-vpcconnectivity-applications-with-amazon-vpc-lattice

The deployment process will take about 10 - 15 minutes, and you will see that our microservices can communicate.

Bug Alert: there's a missing step in the deployment instructions; these two lines will make the deployment fail:

```
export TARGETCLUSTER1={TARGET_GROUP_ARN}
export TARGETCLUSTER2={TARGET_GROUP_ARN}
```

You need to change these exports using values from



When the CloudFormation deployment finishes, you should have these CloudFormation stacks:

Stac	ka (14)			Vehiculation	C Freite Spinse Statusties	Greate stant. *
Q)	Nari ku sasak kuring			Allve.	Ven second	(1)0
	Mark room	Ustan	Constant times 9	Description		
	utto reitra	O CARATE COMPLETE	2014-04-101258-48 UTC-6200	Amazon VICLASSO - Road	ng cón Rgunatian.	
	other details advolutions	CONTANT, COMPLETE	2014-04-101249.591/70-1200	Avector VPC Lattice - EKSY	PCs Service Network Associations	
0	Internetorgen	COLUMN CONNELTS	3034-04-1813-44198-UTC-5230	Aroston VPC Lattice - VPE L	athine Tanget Stronge (Landada Functions and Autochooling group)	
	Labor and share	OCHATLING IT	2004-04-1012/38//SURC-8200	America VPCLame - VPCL	altina Selvines	
P	entiti il entit attes. arme entititare spitter-gentrer se- armelle	O CHEATE, COARNETE	2024-04-1012;01;44UTC-8200	Well-ooks for serviceaccount	"Grand and rearised by dea	1 (
ō	eutlichend Attes erste volkomen gebre gebieg we- soweite	CORNT, UPPLOTE	2024-04-1011.58.35 UTC-8200	AM role for servicescourt	JAnna Zaucash shi councer, (nasang sug nasadag pi gen	AC.
	Hutbible berginging og Saldhint	O CHEATE, COMPLETE	2024-04-10 10:54 #1 UTC+8200	ERS Managert Roders (12)-1 a	classe. Tailori (iz natici) by (disciti)	
	(Inclusion for gamp rate for such that	O'CREATE, COMPLETE	2014-04-10 10:03 H9 L/IC-8200	ERS Managed Rocks: (55H a	status failed (denoted by over2)	
0	weise application	GOMAN, COMMENT	2024-08-10 10/46/12 U/IC-8200	Armstein VPC Later - NML	ueriteta Application	
9	which shared-barre	G CALATE, 2004PLETE	3034-04-10.10-01.07 UPC-8300	EXCLASSING Medicated VPC	No., dollared 305 (cost (costs) and coaraged by start (
	mint date (while	OCHARTE CONNERS	2024-04-10 1045-38 Line-6200	ERS cluster Elizabet VPC	yse, deduated UUC tases (consteal and managed by elect)	
	mg.accidation	CANATE COMMENTS	3034-04-1010/3K281URC+6200	Aniation VPC Labore - Auto	scaling prove Application	
	10102-00349-5	OCHATLOURIES	2024-04-10 10 28:19 L/TC-5200	WHEEH THE LARGE HEAH	13	
ō	Detroite	OCHATE COMPLETE	2023-04-271198-891-70-0200	This stack metaday measure	insuited to deproy AMS CDE apprints this environment.	

Let's see the resources created to describe them. First, the service network:

erv	ice-network							Last forched test roll light	C Atlan
en	ice network details								
mk	a novel name a novel n 13 nadata/6/1016		Series estruct 0 $\mathcal{B} = 0$ ertfaket2stie	601		Des trains Ayré 10, 2024, 10:28-2	8 ((715-92:00)	Care last rest/field April 10, 2024, 10,28,28 0/10 -02,60	
5.	n witwolk MNi mawitwpk-Witzczy Amir 2.554	25/76/314 similarite	u#/++0x5340x1231bd965						
		Invine	and the second second				9	TPC analistican	
4									
			4					3	
erv	to essociations (1)	eine (Anno	4 ••••••••••••••••••••••••••••••••••••	ng.				3 (7) Allem + (4)	aga picettin
ers	na anacticities (1) foe associations (4) set of the set of the set of foe intervention of the set of the	ellere (Ajana uner (d) funtanta (a	4 Northerny marries (1999), 2019 (1999)	ne -				3 [0] [Allers +] [4	un materi
ers	to association (if)	anteres () Apparta () anteres (all Parta anteres dan • ,) ADM	4 manual manag ranna atta ta mana * : tata	Nep V	territor torre	w) Association tags	* Gamby	3	ram posicititan
ers	A musicipation of the second s	инин (Адаан (1999) од Алаан (1999) • Ала (2 Алан (2 Алан	4 rearising manager remove while the second * 1 states © hotor	100	terobe same	₩.) Association tage Tage	* Genelay Intervision	(*) ((1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
in in its second	termentations versions and for associations (1) association to more to ASSNT 12012201 more to ASSNT 12012201 more to ASSNT 12012201 more to ASSNT 12012201	анта Алана ната се попатила • али С яза С яза с али	4 Herestanding manager Herestanding the serveral V Hadres Orthogo Orthogo	5 Mai 1	Mercico Norse merced (merced)	w Januaristica tago E tago E tago	 Giannéky metgyt szülte tisztorotote 	3 () Notest + () * Data stationer Aper 10, 2014, 12 Mol 31 (07-0132) Aper 10, 2014, 12 Mol 31 (07-0132)	1911 (1914 (1914) C + ->
iers	An anno latinos	• 2001 • 2001 • 2001 • 2001 • 2001 • 2001 • 2001	4 Northang mening * Nature © Alter @ Alter @ Alter	Nep N	Mercico Naree accurati accurati accurati	9 Association tops Tops Tops Tops	 Column by Barcoro Prise Solution Prise Solution Prise 	3 * tan sambur April, 200, 12:000 price and April, 200, 12:000	900 000-0000 (+ >

As you can see, four services are associated; you can also see VPCs associated with the service network:



Now VPC Lattice target groups:

Our Lambda, Autoscaling group, and EKS are added as targets, and like ELB target groups, you can see metrics and define health checks.

Targ	nt groups (1/4) entertaije provinsion	de las		Anna				6				<u>_</u>		Action *	Death lan	
9	ad terminant by ethility	e ar big													- 63	1) B
	Rate	\mathbf{x}	Jan .		1010	*	Pet	$\hat{\pi}_{i}$	Protocol +	targettype v	Service 12 T	WYC:ID	+	Walden type	(π)	mis outs
Π.	land do target		(P Abi		(Chifty					Tantolik	m 01040404-					April 10,252
3	Interferenced defailed		(3 AM		Quite		100.00		4873F		In CASE AN	The state in the second second	- 52	894		April 10, 241
	Musichard defail		(S ANI		() hits		0081		64739			We observe the second	63	IFV4		Auri 10, 262
	PROTECT.		(9 Am)		Girm		100		10710	Industri		ver comparisonshipsterich	- 12	1744		April 10, 281
yet	grsup: kBs-fronte	n¢-de	hault .		-											G
yet Istal	group: kös-fronte s tegets	në-de ath c	laulti Hustoria		e											G
rget Istal Heal	grsup: kBs-fronte b Tegets th check settings	nd-de addi ci	rault Heathering		6 - 10 Tex - Appl 2 and 7 by	en tañal	their einden		*							Q 2
Heal	grsup: k0x-fronte b teget: th check settings settictures productory shocks	nd-de addi ch	tault Halt Pastaring orth scaling to fix of	1 1 1 1	e - 1: The significant for manual - 194	et is fait	their disks.			er.		Part				G .
rget Detail Heal	grsup: kBs-fronte • Teget:	nd-de add co	laulti III. Pastharing orth asselling in Two	1 1 1 1	e et te system to ment 199	et 5 he	their distan			er.		Part 0000				G .
rget letel Heal for an	grsup: kBs-fronte b Tegen th check settings which settings at recent	nd-de addi ch	Handbarnen Handbarnen Handbarnen	1. 1. 	et in the against for second repr activy threehold access the bandle of	etter to their	their etallis annes			ity meetly trained constants halfs the	t biom	Port 2000 Trinout				0
rget Tetal Heal Notes Tetas retur	group: Allo-fronte to trape: th check settings electrone settings all return all return all return	nd-de alth ch	hužt Hestarny	1 12 14 14 14 14	er or the significant for control or the significant or the sound of the start of the sound of the start	etter fan Frank	their station			di. Mesety teatiod seconds both (bat	s baiseys.	Part allos Trynout Sacont				0 Lde

Note that to register our targets managed by EKS clusters, we had to deploy the Gateway API Controller Class into the cluster and register the service using the configuration deployed with the commands:

```
kubectl config use-context cluster1
kubectl apply -f ./vpc-lattice/routes/frontend-export.yaml
kubectl config use-context cluster2
kubectl apply -f ./vpc-lattice/routes/backend-export.yaml
```

Last but not least, let's see the defined services. You can access them using the DNS domain name defined by VPC Lattice

A SPC Laboration in the Anthen	a sease. Stating, and see sharing the tasks	on traffic to assess have been been been	and the local distance of the		was t	his article useful for vou?
Q instreaments for	138-0 o 16					······································
B Nerer	• Driarightee	a lan	W Sides	V Domaticaster V Cost	intern Kerne	
E mysted		(2) APRI	Quine	Ø www.wertset		
S month		(5 sm	Gum	Ø ereisebattian		
El mentes		C Am	Glasse	🗇 ++ruit#2.0##18\7		γραί
(7 service)		(3 Am	(C) ACTIVE	di emini 0.72m -		100.
trylce: service3	rvet analatura — Analing	Acces Verteing	Surry by:			I was expecting something
service: service3	nyu's constaines — Bauing	Acces Mantanag	Surry Ugr	and the second s		I was expecting something
service details	nvelt anatolites 🕺 Bauling	Acces Viceboog	Surry tyr		274	I was expecting something different
Invice service3 Invice details Service details Service 3 Invice 0 Invice 0 Invice 0	ment analistan kaning	Acces Mentantes Status Schilter Charter 2 Schilter	Starrey Ugo	Press control April 10, 2004, 1255/23 0,070-02 Marine (page 17) Cl 2004/1210/0402/04404	2-94	l was expecting something different
trvice: service3 bilds service Service details Service details Service 3 Service 8 Service 8	nvoit sostatus - Asutog	Access Mentioning Series Const C Const C Const C Const C	Surry tyr	an Free Constant (1) State Constant (2) State Const	204	l was expecting something different
tendes services tendes services Service details Service details Service 0 B occurses Service 0 B occurses Service 0 B occurses Service details	nveri anatolana (Acces Venturing Dense O Arine Dense (7) D Seeksuranter	Surg by	a 3 santstucinde/ceeta eesta 20 20 129 129 129 129 pancaran		l was expecting something different
tendes annifets tendes Service details Service details Service details Service details Service details Service details Service details Service details Service details Service details	nnevit anastatus – Pauting antif avant 25040077054-anastr	Acces Westering Source Oblights Description Descriptions Constate (chame)	Surray bar	Q. Sauristicupid, Keela providencia processi processi processi		l was expecting something different

You can find the complete list of domain names defined by looking at the Outputs of the CloudFormation stack named "lattice-services":

	ration 3 Statu 3	11	lattice-services									0.3
5	tacks (34)						Delata Baj	daina	Situeli actionar 🕈	649	ia star	
1	Ew to start name		Just 19's Excell Record	rize 0	htpats Parameters Template	Chi	nge auto 000 type - Now					
1	italas.		Outputs (II)								E.	3
	0.0		Q. Sand-system							10.4	5	0
	Amanda		***		talas .	1	Description	÷	Topert same			
	Intra-many JU-I-I-D UNALITI-DOX ©CHINE CONFLITE		Dervice 1		among ng katuran west 2.564950707834.semina/pen- Ga Y28586aaa80778		WC Latter Service 1 (6)					
	withe do-spe excellent		Service/Demonstration		antria). GuMUNdhaudATTA ANTALAni Latian. Maanatta Latama		WC Latter General Thomas Name					
	Netton Regets		Service2		annaertype ratt trans-seed. 2-56 attist/67161-65 anniertypen. Geologi Tradiello attist.		WK; Lathón hannan 2 (B).					
	CONVERSION IN		Service20enant/seter		antikala Gentin Tarkell with A. Zolf Zolf Anno. Batter- Balaan muti Antami		WC Lation Service 2 Stream Barrow					
	CRARCSCHAUT		far-years.		ancani ya fattama weti- 2 564950% tata sever two 011546564970 ant		WCLatter Server 510					
	lanonrikosarovit spitori. yronny api sentraller Josa os. 10 (co) (ac ch2-coo)		fer van Kösmanstame		annika 3 00 10 000 00 11 2 anil 7 2 00 10 0 anni Int Resourcements 2 2 0 anni		VPC Lattice beaute & Domain Ranie.					
	Score (concise		lamics4		arcancep: Anti-pas-web 2164063767854:service/re- 061131ew/dele5/074		WCLattor Gevin 410.					
	Bearing Bearing and Augusta		far vir still beruperkaras		errited. On 1510 Automatication (1901) Biology, Larrow,		WCLattice Service 4 Deviate Raine					

Each service also has its routing; in this case, you can see that /backend path for service3 forwards to cluster2, while /lambda forwards requests to the lambda application:

Services (1/16)			and the second second					(C) #1806	· United and
1. The second ly second	e d by								1.1.1.1
	•	+ 1.446	- 1 - 1000	1			* ********** *	0443 ×	last model
O sectori		0 MK	(2 trem	() berrouk (BUTS	u.,)		2000/2011/00/00/00	menoranta	Aurel 10, 10035, 17700
a mini		(5 AM	() total	0 mm0-mm	e		200121021426002503	manoremia	April 10, 2018, 12:30
		15 Aller	Sec.	B arrestant	et		210912-02214790/07147	manufactor	April 10, 1614, 1221
C mmt		(D. 140)	(D +++=	() investigation			20012102140000000	manoratela	April 11, 1634, 17,28
teau larestation reling Interestation of the reality Π	t annätten som för	Autor Hamon	y 2007g Tap					- March Inter	0 100 Anno
Constraints the constraints	en antraciante en escala	with path condition June Iron	entral to torne usin, Add	and another static artiges	Accordings, for public of TP and	test and header are a communicate	which in the second stage to the	All sectors II	
other states		Paper	e Mart		745414300		144		
Second Second Second Second	e de gene	office			formation to period 10	10.00%	3 P		
Berni -		denotities:				1004		. Posts	
factored ages periods (1 Pain Profile (A	and and provide stations			Terminita International Column	43	1.7	
weeks and second		A Date Dates of the				Thrandta		1.00	
						10110			

Now that you have a deployed infrastructure, feel free to experiment and modify the behaviour of your application and environment (why don't you try IAM authentication between services?).

This is only a starting point, and you can also find an excellent AWS workshop with a good walkthrough here.

Last but not least: is VPC Lattice the right

The correct answer is, as always: "It depends". Let's impact on our design.

The first is the mandatory **one-to-one association k Network**. Once you define an association, you cann other service networks, so you need to plan the imp

You cannot share services between different region

regional construct: you'll need to use a hybrid approach, resorting to traditional" connectivity methods, like Transit Gateway Peering and VPC Peering.

On the other hand, there are great **benefits**: you can free service owners to configure and offer by themselves their components while keeping centralized control in a complex environment.

We didn't have a look at IAM policies, but **implementing IAM Authentication and** Authorization is the key to a secure microservice implementation.

VPC Lattice also offers a complete service mesh solution because it can link EC2, EKS, ECS, and Lambda workloads.

Cost is another important factor: **as your service mesh grows, costs increase proportionally**.

You pay 0.025\$/hour for each service. If you have 10 services you pay 182.5\$/month. A different approach can have a smaller impact on AWS billing for complex architectures with hundreds of microservices.

That's all for today!

Microservices aren't simple: they can increase the overall complexity of the architecture and require good planning and management over time.

Have you already had the chance to experiment with VPC Lattice? What are your thoughts about this new approach?

Let us know in the comments!

About Proud2beCloud

I was expecting something different

🥠 Made with Hotjar

Yes!

Was this article useful for you?

Proud2beCloud is a blog by beSharp, an Italian API in designing, implementing, and managing complex advanced services on AWS. Before being writers, w with AWS services since 2007. We are hungry reade seekers. On Proud2beCloud, we regularly share our insights, in-depth news, tips&tricks, how-tos, and m the discussion!

Was th	nis article useful for you?
$(\bigcirc$	Yes!
\bigcirc	I was expecting something different
🥠 Made	with Hotjar



Damiano Giorgi

Ex on-prem systems engineer, lazy and prone to automating boring tasks. In constant search of technological innovations and new exciting things to experience. And that's why I love Cloud Computing! At this moment, the only "hardware" I regularly dedicate myself to is that my bass; if you can't find me in the office or in the band room try at the pub or at some airport, then!

Copyright © 2011-2024 by beSharp spa - P.IVA IT02415160189