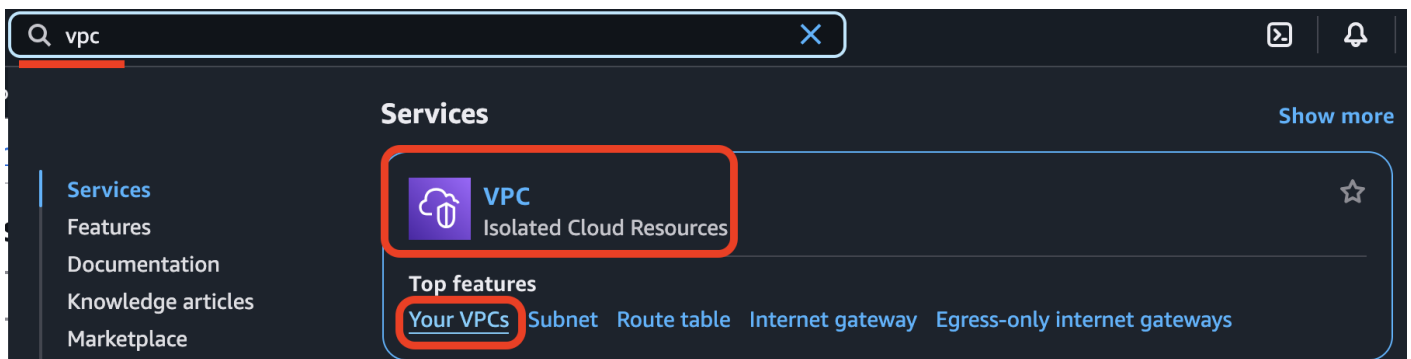


0. How to Find Required Parameters

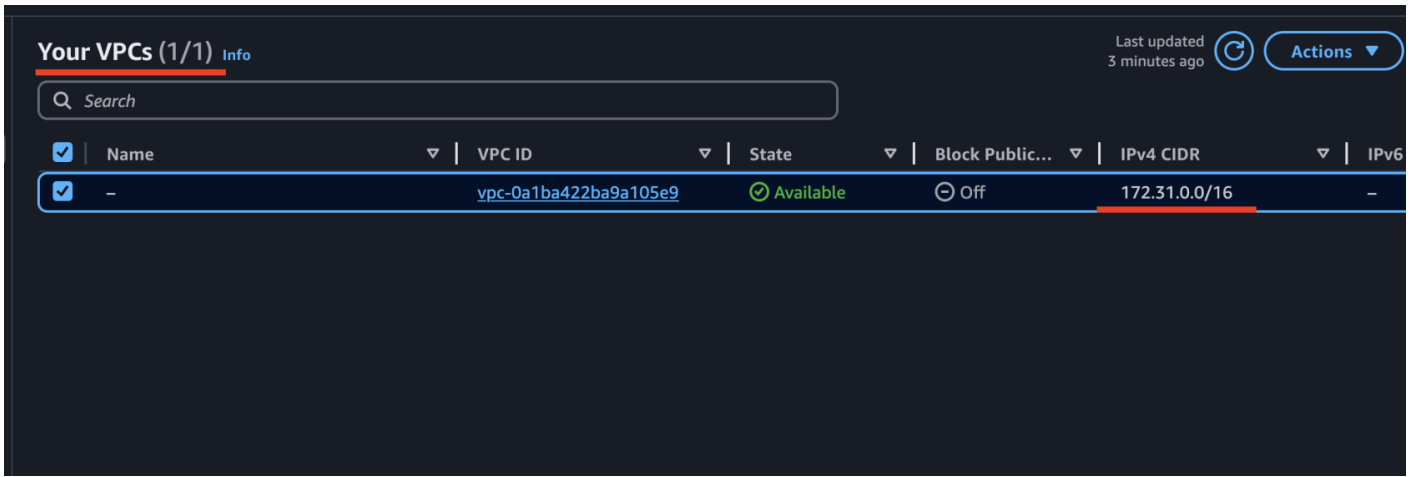
To properly deploy BookStack, you need to provide the following network parameters and certificate ARN:

1 VpcCidrBlock (CIDR block for the VPC)

- If you are **creating a new VPC**, use `10.0.0.0/16` as the default value.
- If you are **using an existing VPC**, retrieve the CIDR block:
- Open **AWS Console** → **VPC** → **Your VPCs**

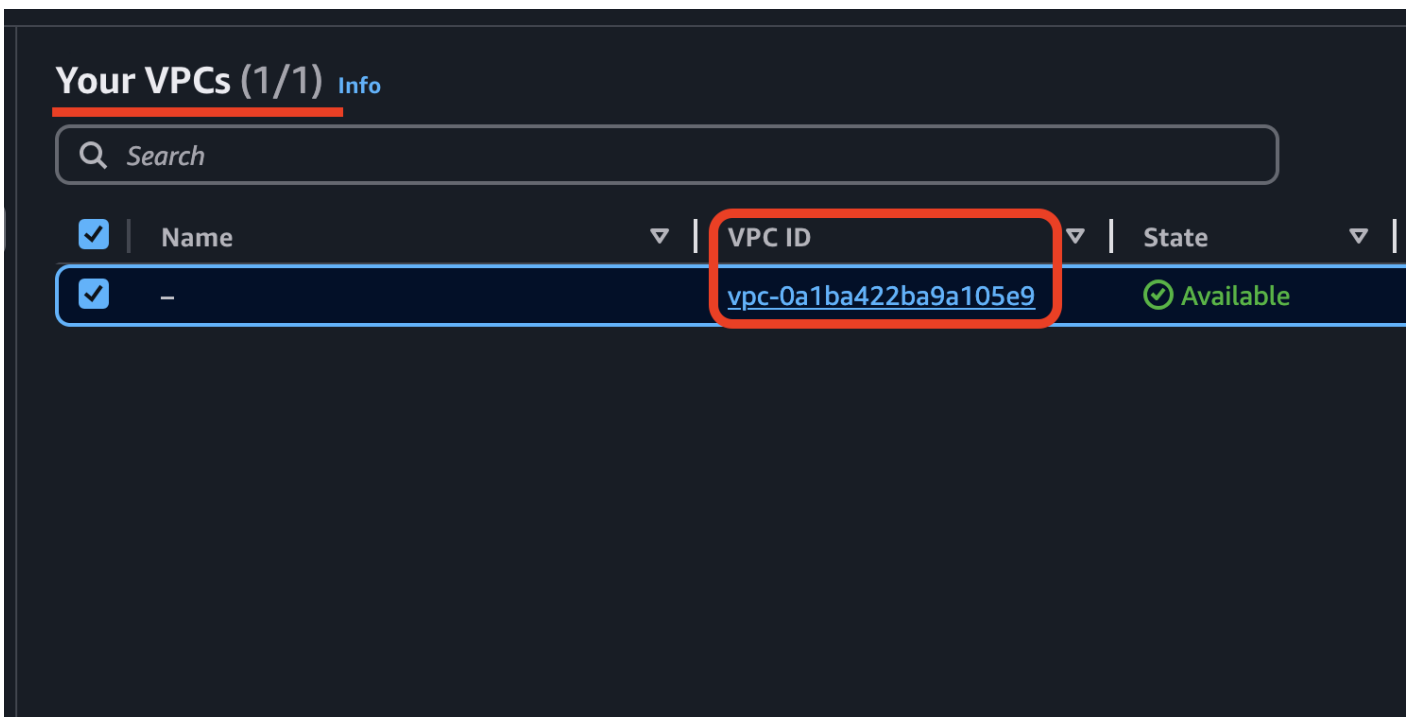


- Locate your VPC and copy the **IPv4 CIDR** value.



2. VpcId (VPC ID)

- Locate your VPC and copy its **VPC ID** (e.g., vpc-0a1ba422ba9a105e9).



3. Subnet1Id & Subnet2Id (Subnet IDs)

- Open **AWS Console** → **VPC** → **Subnets**
- Select your VPC, and at the bottom panel, navigate to the **Resource Map** tab.
- Here, you will see a list of all subnets associated with your VPC.
- Choose two **private subnets** (preferably in different Availability Zones) and copy their **Subnet IDs** (e.g., subnet-040155a08a9508bb6, subnet-02e4a590db71371f9).

The screenshot shows the AWS Management Console VPC dashboard. On the left is a navigation menu with categories like 'Virtual private cloud', 'Security', and 'PrivateLink and Lattice'. The main area displays 'Your VPCs (1/1)' with a table listing VPC details. Below this, the 'Resource map' tab is active, showing a diagram of the VPC resources. A VPC with ID 'vpc-0a1ba422ba9a105e9' is shown, containing two subnets: 'us-west-1b' (subnet-040155a08a9508bb6) and 'us-west-1c' (subnet-02e4a590db71371f9). Three route tables are also listed: 'wiki-test-public-rtb', 'rtb-0e7c6421f1275a72c', and 'wiki-test-private-rtb'. The subnets and route tables are highlighted with red boxes.

⚠ Important Notice! Ensure that the region of your resources matches the deployment region in CloudFormation. If you select resource IDs from **Region A** but deploy in **Region B**, you will encounter an error stating that the specified resources do not exist. This happens because each AWS region has its own unique set of resource IDs.

4. Obtain an SSL Certificate (if you don't have one):

- Navigate to **AWS Certificate Manager (ACM)** in the AWS Management Console.
- **Request** a new certificate by selecting **“Request a public certificate”** and click **Next**.

The screenshot shows the 'Request certificate' page in the AWS Certificate Manager console. The breadcrumb trail is 'AWS Certificate Manager > Certificates > Request certificate'. The page title is 'Request certificate'. Under the 'Certificate type' section, there are two radio button options: 'Request a public certificate' (which is selected and highlighted with a red box) and 'Request a private certificate'. Below the options, there is a note: 'Requesting a private certificate requires the creation of a private certificate authority (CA). To create a private CA, visit AWS Private Certificate Authority'. At the bottom right, there are 'Cancel' and 'Next' buttons.

- Follow the steps to validate your domain using **DNS validation (recommended)** or **Email validation**.

[AWS Certificate Manager](#) > [Certificates](#) > [Request certificate](#) > Request public certificate

Request public certificate

Domain names Info
Provide one or more domain names for your certificate.

Remove
 Remove

[Add another name to this certificate](#)

You can add additional names to this certificate. For example, if you're requesting a certificate for "www.example.com", you might want to add the name "example.com" so that customers can reach your site by either name.

Validation method Info
Select a method for validating domain ownership.

DNS validation - recommended
Choose this option if you are authorized to modify the DNS configuration for the domains in your certificate request.

Email validation
Choose this option if you do not have permission or cannot obtain permission to modify the DNS configuration for the domains in your certificate request.

- Select `ECDSA P-256` as the key algorithm. This is equivalent in cryptographic strength to **RSA 3072** but provides better performance. If `ECDSA P-256` is not supported by your use case, you can use `RSA 2048` instead (though it is less efficient). Create the tag with **Key=Name**, **Value=bookstack** (or any other meaningful name that helps you recognize it)

Key algorithm Info
Select an encryption algorithm. Some algorithms may not be supported by all AWS services.

RSA 2048
RSA is the most widely used key type.

ECDSA P 256
Equivalent in cryptographic strength to RSA 3072.

ECDSA P 384
Equivalent in cryptographic strength to RSA 7680.

Tags Info

Key	Value - optional	
<input type="text" value="Name"/>	<input type="text" value="bookstack"/>	Remove

[Add new tag](#)

You can add up to 49 more tags.

Cancel Previous Request

- Once the certificate is issued, copy its **ARN** and use it in the **SSLCertificate** parameter during deployment.

2ec1e07c-bd20-4419-9857-84e5150f20f3

Certificate status

Identifier

2ec1e07c-bd20-4419-9857-84e5150f20f3

ARN

 arn:aws:acm:us-west-1:████████████████████:certificate/2ec1e07c-bd20-4419-9857-84e5150f20f3

Type

Amazon Issued

⚠ **Important Notice!** Ensure that the certificate is created in the **same AWS region** where you are deploying the CloudFormation stack. If the certificate is in a different region, the ALB will not be able to use it, and the deployment will fail.

Revision #8

Created 6 March 2025 07:47:20

Updated 17 March 2025 08:35:59 by dmytro