

Private Computation: Guide to answering AWS pre-check questions

AWS network mode

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>
2. In the navigation bar, use the **Region** selector on the top right to select your Region.
3. On the Amazon EC2 console dashboard, look for **Supported Platforms** under **Account Attributes**.

The screenshot shows the AWS Management Console interface. The top navigation bar includes the AWS logo, 'Services', a search bar, and the region selector set to 'N. Virginia'. The left-hand navigation pane shows the 'EC2 Dashboard' selected. The main content area displays 'Resources' for the 'US East (N. Virginia) Region' with a table of EC2 resources. The right-hand pane shows 'Account attributes' with a red box highlighting 'Supported platforms' and 'Default VPC'.

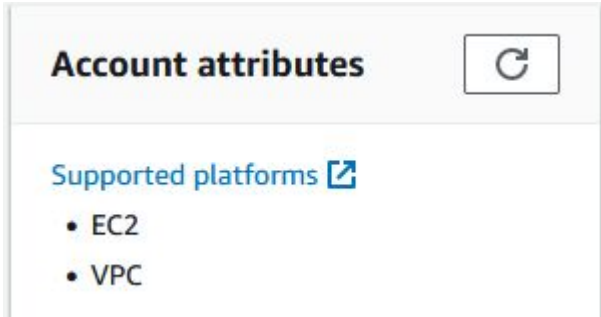
Resources

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

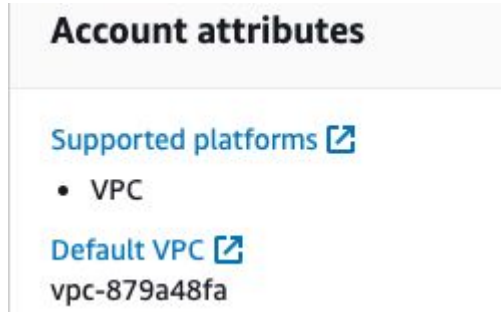
Instances (running)	1	Dedicated Hosts	0	Elastic IPs	0
Instances	1	Key pairs	0	Load balancers	0
Placement groups	0	Security groups	2	Snapshots	8
Volumes	2				

Account attributes

- Supported platforms
 - VPC
- Default VPC
 - vpc-879a48fa



If you have “EC2” in supported platforms.
Means your account in the region is using **EC2-Classic**.



If the Default VPC is not “vpc-XXXXXX” like
“None”, then means you don’t have
Default VPC defined.

Check VPC numbers

The screenshot shows the AWS Management Console interface. In the top navigation bar, the 'N. Virginia' region is selected and circled in red. A red arrow points from this region selector to the 'VPC Dashboard' link in the left-hand navigation menu, which is also circled in red. Another red arrow points from the 'VPCs' resource card in the 'Resources by Region' section to the 'N. Virginia' region selector. The 'Resources by Region' section displays a grid of VPC resources for the US East region:

Resource Type	Count
VPCs	1
NAT Gateways	0
Subnets	6
VPC Peering Connections	0
Route Tables	1
Network ACLs	1
Internet Gateways	1
Security Groups	2

The 'VPCs' card is circled in red. The right-hand sidebar contains sections for 'Service Health' (showing 'Amazon EC2 - US East' as 'Service is OK'), 'Settings' (with links for Zones and Console Experiments), and 'Additional Information' (with links for VPC Documentation, All VPC Resources, Forums, and Report an Issue).

Default limit VPCs per region is 5, this could be increased using the [Amazon VPC limits form](https://docs.aws.amazon.com/iam/latest/userguide/iam_limits.html)

<https://docs.netgate.com/pfsense/en/latest/solutions/aws-vpn-appliance/aws-service-limits.html>

Check access to Private computation resources - S3

1. Login to your AWS.
2. Open IAM Policy: Simulator <https://policysim.aws.amazon.com/home/index.jsp?#roles>

Check Private Computation S3 access

1. Choose a Role that contains **AmazonS3FullAccess**.
2. Select service => **S3**
3. Select Action => **ListBucket**,
GetObject
 - a. Put
`arn:aws:s3:::one-docker-repository-prod` to bucket`
 - b. Put
`arn:aws:s3:::one-docker-repository-prod/private_lift/lift/latest` to object`
4. Click `Run simulation`
5. Check if the permission shows **"allowed"** or **"denied"**.

The screenshot shows the AWS IAM Policy Simulator interface. Red circles and arrows highlight the following elements:

- Selected role:** A red circle around the role name, with an arrow pointing to the **AmazonS3FullAccess** role in the IAM Policies list on the left.
- Service:** A red circle around the **Amazon S3** dropdown menu.
- Action(s):** A red circle around the **2 Action(s) selected** dropdown menu.
- Run Simulation:** A red circle around the **Run Simulation** button in the top right corner.
- Global Settings:** A red circle around the **Global Settings** link.
- Simulation Resource:** Two red circles around the simulation resource input fields. The first is for the **ListBucket** action, containing `arn:aws:s3:::one-docker-repository-prod`. The second is for the **GetObject** action, containing `arn:aws:s3:::one-docker-repository-prod/private_lift/lift/latest`.

The **Action Settings and Results** table shows the following results:

Service	Action	Resource Type	Simulation Resource	Permission
Amazon S3	ListBucket	bucket	bucket	allowed 1 matching statements.
Amazon S3	GetObject	object	object	allowed 1 matching statements.

Check access to Private computation resources - ECR

1. Login to your AWS.
2. Open IAM Policy: Simulator <https://policysim.aws.amazon.com/home/index.jsp?#roles>

Check Private Computation ECR access

1. Choose a Role that contains **AmazonECSTaskExecutionRolePolicy**.
2. Select service => **Elastic Container Registry**
3. Select Action
=> **BatchCheckLayerAvailability**,
BatchGetImage, **GetDownloadUrlForLayer**
 - a. Put
`arn:aws:ecr:us-west-2:539290649537:repository/one-docker-prod` to Simulation Resource`
4. Click `Run simulation`
5. Check if the permission shows "**allowed**" or "**denied**".

Policies [Back] [Create New Policy]

Selected role: [Redacted]

AWS Organizations SCPs [x] Service control policies (SCPs) applied to your account can impact your access to AWS services. [Learn more.](#)

IAM Policies [Filter] [x] **AmazonECSTaskExecutionRolePolicy**

Custom IAM Policies There are no policies to display!

Permissions Boundary Policy You can simulate a maximum of one permissions boundary policy per user or role. There are no policies to display!

Custom IAM Permissions Boundary Policy

Policy Simulator [Amazon Elastic Container Registry] [Action(s) selected] [Select All] [Deselect All] [Reset Contexts] [Clear Results] [Run Simulation]

Global Settings

Action Settings and Results [3 actions selected. 0 actions not simulated. 3 actions allowed. 0 actions denied.]

Service	Action	Resource Type	Simulation Resource	Permission
Amazon Elastic Container Registry	BatchCheckLayerAvailability	repository	arn:aws:ecr:us-west-2:539290649537:repository/one-docker-prod	allowed 1 matching statements.
Amazon Elastic Container Registry	BatchGetImage	repository	arn:aws:ecr:us-west-2:539290649537:repository/one-docker-prod	allowed 1 matching statements.
Amazon Elastic Container Registry	GetDownloadUrlForLayer	repository	arn:aws:ecr:us-west-2:539290649537:repository/one-docker-prod	allowed 1 matching statements.