

RVOC Engine

AWS Pre-requisites
Technical data sheet

Table of contents

Table of contents	2
RVOC Engine AWS Pre-requisite Technical data sheet	3
Sign up for an AWS account	4
VPC Setup	5
Introduction to VPCs	5
Key Concepts	5
VPC Costs	6
Free VPC Components	6
Cost-Incurring Components	6
Determine your IP address ranges	7
Select your Availability Zones	8
Standard Mode VPC Setup	9
High Availability Mode VPC Setup	12
Deleting your VPC	15
Amazon SES	16
Setting Up Amazon SES with Domain Authentication	16
Amazon EC2 - Elastic IP	20
Amazon S3 Bucket	21
Frequently asked questions	24
1. How to calculate the expected data egress costs for my RVOC engine?	24
2. Why does an RVOC engine require a public and private subnet?	24
3. How many private IP addresses does my RVOC engine use?	24
4. What is the effect of the use of AWS Global Accelerator on my latency?	25
5. Why does RVOC engine require AWS global accelerator in case of High Availability.	25
6. How many Elastic IP's does RVOC require?	25
7. Why does SMTP over port 25 not work?	25

RVOC Engine AWS Pre-requisite Technical data sheet

All instructions in this guide are specifically to host the RTS RVOC Engine on Amazon Web Services. The AWS resources which will be set up will not be fit for any other purpose than running the RVOC Engine, in case you need to host multiple applications within the AWS account please involve a cloud expert to ensure compatibility of the Account setup between the different applications. Your organization might require additional security measures which are not covered in this datasheet. Before making cloud deployments, always involve your security team.

This manual will guide you through setting up an AWS account. It's designed for users new to AWS and provides step-by-step instructions for both RVOC Engine standard and RVOC Engine High Availability configuration.

Before installing RVOC Engine you require the following to be setup on AWS:

- AWS account (with administrator rights)
- VPC
 - One public subnet
 - One private subnet NAT Gateway / internet connectivity)
- (optionally) Email sending service (AWS SES or any other SMTP compatible service)
- At least 2 Elastic IP's available for a non-high available system (note that this might require an AWS Service limit increase)
- AWS S3 bucket hosting the software packages

For any questions related to configuring your AWS account / AWS services please contact AWS support. RTS intercoms support can only support with the actual RVOC engine.

Sign up for an AWS account

If you do not have an AWS account, complete the following steps to create one.

To sign up for an AWS account

1. Open <https://portal.aws.amazon.com/billing/signup>.
2. Follow the online instructions.

Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

When you sign up for an AWS account, an AWS account root user is created. The root user has access to all AWS services and resources in the account. As a security best practice, assign administrative access to a user, and use only the root user to perform [tasks that require root user access](#).

AWS sends you a confirmation email after the sign-up process is complete. At any time, you can view your current account activity and manage your account by going to <https://aws.amazon.com/> and choosing My Account.

VPC Setup

Introduction to VPCs

A VPC is a virtual network dedicated to your AWS account. It's logically isolated from other virtual networks in the AWS cloud. You can think of it as your own private space within AWS where you can launch AWS resources, such as EC2 instances, or in our case an RVOC Engine

Key Concepts

- **Subnet:** A range of IP addresses in your VPC. Subnets can be public or private.
- **Public Subnet:** A subnet whose resources can be accessed from the internet.
- **Private Subnet:** A subnet whose resources cannot be accessed directly from the internet.
- **NAT Gateway:** A Network Address Translation (NAT) gateway enables instances in a private subnet to connect to the internet or other AWS services, but prevents the internet from initiating a connection with those instances.
- **Availability Zone (AZ):** Distinct locations within an AWS region that are engineered to be isolated from failures in other Availability Zones.

VPC Costs

While Amazon VPC provides the foundational networking infrastructure for your cloud intercom system at no additional charge, it's important to understand the cost implications of various VPC components and features.

Note that the below list is not complete, it only focuses on the VPC components deployed within this guide.

Free VPC Components

- VPC Creation and Management: Creating and maintaining VPCs incurs no cost
- Subnets: Subnets within your VPC are free to create and manage
- Route Tables: Custom routing configurations within your VPC
- Security Groups and NACLs: Firewall and access control features
- Internet Gateways: Components enabling internet connectivity
- Gateway endpoints: For S3

Cost-Incurring Components`

NAT Gateways

- Hourly charges
- Data processing

Inter-AZ data transfer:

- Data processing

Data egress (internet out):

- Data processing

Please see AWS Pricing page for current pricing:

<https://aws.amazon.com/pricing/>

Determine your IP address ranges

The resources in your VPC communicate with each other and with resources over the internet using IP addresses. When you create VPCs and subnets, you can select their IP address ranges. When you deploy resources in a subnet, such as EC2 instances, they receive IP addresses from the IP address range of the subnet. For more information, see [IP addressing for your VPCs and subnets](#).

RVOC Engine deployments require at least /27 subnets (this include room for future updates of the product).

Example:

VPC CIDR: 10.10.0.0/23

This provides 512 total IP addresses

Sufficient space to contain your required subnets with room for expansion

Public Subnet: 10.10.0.0/27

Provides 32 IP addresses (30 usable)

Available range: 10.10.0.0 - 10.10.0.31

Usable IPs: 10.10.0.1 - 10.10.0.30

Reserved: 10.10.0.0 (network), 10.10.0.31 (broadcast)

Purpose: Internet-facing components, load balancers, NAT gateways

Private Subnet: 10.10.0.32/27

Provides 32 IP addresses (30 usable)

Available range: 10.10.0.32 - 10.10.0.63

Usable IPs: 10.10.0.33 - 10.10.0.62

Reserved: 10.10.0.32 (network), 10.10.0.63 (broadcast)

Purpose: Backend services, databases, internal components

Select your Availability Zones

An AWS Region is a physical location where we cluster data centers, known as Availability Zones. Each Availability Zone has independent power, cooling, and physical security, with redundant power, networking, and connectivity. The Availability Zones in a Region are physically separated by a meaningful distance, and interconnected through high-bandwidth, low-latency networking.

Select the region that has the lowest geographical distance from your physical location to minimize latency and improve application responsiveness; available regions can be found at <https://www.aws-services.info/regions.html>

RVOC Standard deployment

A RVOC Standard deployment only requires a single Availability Zone to be selected

RVOC High Availability deployment

A RVOC High Availability deployment requires 2 Availability Zone within the same region to be selected

Example:

For your production facility in Washington DC, you'll want to select an AWS region that provides the lowest latency and highest reliability for your cloud intercom system.

*Recommended AWS Region: US East (N. Virginia) - **us-east-1***

This is the ideal choice for your Washington DC location because:

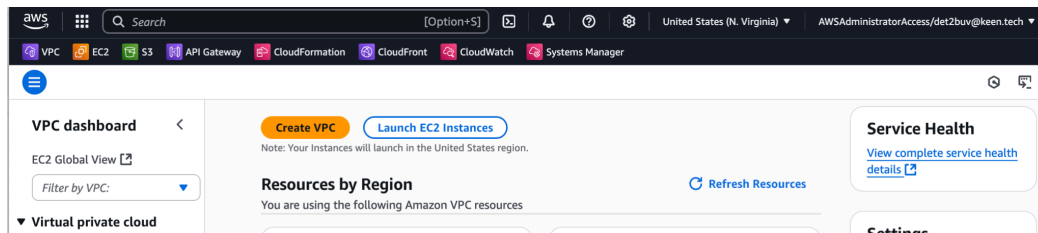
- It's physically the closest AWS region to Washington DC (approximately 90 miles away)*
- The minimal geographic distance will provide the lowest possible latency*
- This proximity ensures voice communications remain clear with minimal delay*
- The N. Virginia region has extensive connectivity options to the DC metro area*

Standard Mode VPC Setup

This section covers setting up a VPC with one public and one private subnet in the same Availability Zone using the VPC Wizard.

Note: For high availability deployments please go to the next section.

1. Log in to the AWS Management Console.
2. Navigate to the VPC service and the planned region



3. Select "Create VPC."
4. Choose "VPC and more"
5. Configure the VPC with a name, CIDR block (IP range), 1 Availability Zone, 1 Public Subnet and 1 Private Subnet

... is an isolated portion of the AWS cloud operated by AWS, subject to...

VPC settings

Resources to create [Info](#)
Create only the VPC resource or the VPC and other networking resources.

☐ VPC only ☒ VPC and more

Name tag auto-generation [Info](#)
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

☒ Auto-generate

IPv4 CIDR block [Info](#)
Determine the starting IP and the size of your VPC using CIDR notation.

10.10.0.0/23 512 IPs

CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)

☒ No IPv6 CIDR block ☐ Amazon-provided IPv6 CIDR block

Tenancy [Info](#)

Default

Number of Availability Zones (AZs) [Info](#)
Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1 | 2 | 3

► **Customize AZs**

Number of public subnets [Info](#)
The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0 | 1

Number of private subnets [Info](#)
The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0 | 1 | 2

► **Customize subnets CIDR blocks**

6. Review the subnet allocations to ensure they match your planning

▼ Customize subnets CIDR blocks

Public subnet CIDR block in us-east-1a

10.10.0.0/27 32 IPs

Private subnet CIDR block in us-east-1a

10.10.0.32/27 32 IPs

NAT gateways (\$) [Info](#)

7. Create 1 NAT Gateway and the S3 VPC Endpoint.

NAT gateways (\$) [Info](#)

Choose the number of Availability Zones (AZs) in which to create NAT gateways.
Note that there is a charge for each NAT gateway

None | **In 1 AZ** | 1 per AZ

VPC endpoints [Info](#)

Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

None | **S3 Gateway**

DNS options [Info](#)

☒ Enable DNS hostnames

☒ Enable DNS resolution

► Additional tags

Note without internet connectivity the intercom will not be installed correctly!

8. Review and create the VPC.

Create VPC workflow

⌂ Wait for NAT Gateways to activate 70%

▼ Details

✔ Create VPC: [vpc-0663baa440b7b90ef](#)

✔ Enable DNS hostnames

✔ Enable DNS resolution

✔ Verifying VPC creation: [vpc-0663baa440b7b90ef](#)

✔ Create S3 endpoint: [vpce-0706356565341cbef](#)

✔ Create subnet: [subnet-0dfefde14f9c2a344](#)

✔ Create subnet: [subnet-0e15646bb01566263](#)

✔ Create internet gateway: [igw-093fe9460258d24e5](#)

✔ Attach internet gateway to the VPC

✔ Create route table: [rtb-0353df619ff2124b1](#)

✔ Create route

✔ Associate route table

✔ Allocate elastic IP: [eipalloc-0ff71477fb805572d](#)

✔ Create NAT gateway: [nat-0fc983e8e775a9667](#)

⌚ Wait for NAT Gateways to activate

⌚ Create route table

⌚ Create route

⌚ Associate route table

⌚ Verifying route table creation

⌚ Associate S3 endpoint with private subnet route tables: [vpce-0706356565341cbef](#)

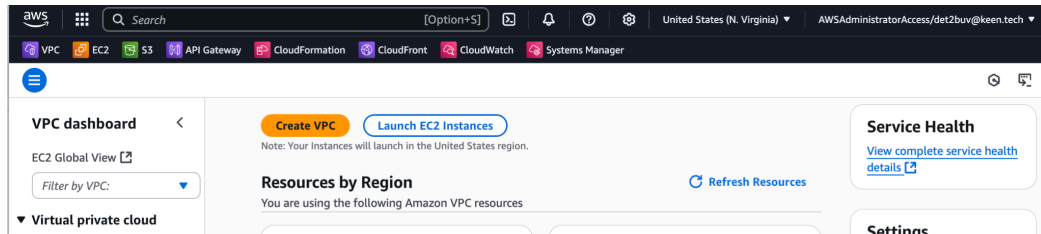
9. Wait for your VPC workflow to complete. Your VPC is now ready for use with an RVOC Engine

Note that the VPC will incur costs (even when not used) due to the resources created.

High Availability Mode VPC Setup

This section covers setting up a VPC with two public and two private subnets across two different Availability Zones using the VPC wizard

1. Log in to the AWS Management Console.
2. Navigate to the VPC service and the planned region



3. Select "Create VPC."
4. Choose "VPC and more"
5. Configure the VPC with a name, CIDR block (IP range), 2 Availability Zones, 2 Public Subnets and 2 Private Subnets

VPC settings

Resources to create [Info](#)
Create only the VPC resource or the VPC and other networking resources.

☐ VPC only ☒ VPC and more

Name tag auto-generation [Info](#)
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

☒ Auto-generate

IPv4 CIDR block [Info](#)
Determine the starting IP and the size of your VPC using CIDR notation.

10.10.0.0/23 512 IPs

CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)

☒ No IPv6 CIDR block ☐ Amazon-provided IPv6 CIDR block

Tenancy [Info](#)

Default

Number of Availability Zones (AZs) [Info](#)
Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1 | 2 | 3

► **Customize AZs**

Number of public subnets [Info](#)
The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0 | 2

Number of private subnets [Info](#)
The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0 | 2 | 4

▼ **Customize subnets CIDR blocks**

6. Review the subnet allocations to ensure they match your planning

▼ **Customize subnets CIDR blocks**

Public subnet CIDR block in us-east-1a

10.10.0.0/27 32 IPs

Public subnet CIDR block in us-east-1b

10.10.0.32/27 32 IPs

Private subnet CIDR block in us-east-1a

10.10.1.0/27 32 IPs

Private subnet CIDR block in us-east-1b

10.10.1.32/27 32 IPs

7. Create 2 NAT Gateways (1 per AZ) and the S3 VPC Endpoint.

NAT gateways (\$) [Info](#)

Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

None | In 1 AZ | **1 per AZ**

VPC endpoints [Info](#)

Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

None | **S3 Gateway**

DNS options [Info](#)

- ☒ Enable DNS hostnames
- ☒ Enable DNS resolution

► **Additional tags**

Note without internet connectivity the intercom will not be installed correctly.

8. Review and create the VPC.

Create VPC workflow

Wait for NAT Gateways to activate

70%

▼ Details

✔ Create VPC: [vpc-0663baa440b7b90ef](#)

✔ Enable DNS hostnames

✔ Enable DNS resolution

✔ Verifying VPC creation: [vpc-0663baa440b7b90ef](#)

✔ Create S3 endpoint: [vpce-0706356565341cbef](#)

✔ Create subnet: [subnet-0dfefde14f9c2a344](#)

✔ Create subnet: [subnet-0e15646bb01566263](#)

✔ Create internet gateway: [igw-093fe9460258d24e5](#)

✔ Attach internet gateway to the VPC

✔ Create route table: [rtb-0353df619ff2124b1](#)

✔ Create route

✔ Associate route table

✔ Allocate elastic IP: [eipalloc-0ff71477fb805572d](#)

✔ Create NAT gateway: [nat-0fc983e8e775a9667](#)

⌚ Wait for NAT Gateways to activate

⌚ Create route table

⌚ Create route

⌚ Associate route table

⌚ Verifying route table creation

⌚ Associate S3 endpoint with private subnet route tables: [vpce-0706356565341cbef](#)

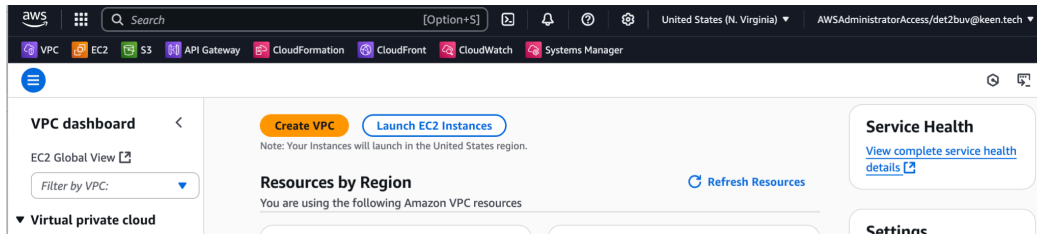
9. Wait for your VPC workflow to complete. Your VPC Is now ready for use with an RVOC Engine

Note that the VPC will incur costs (even when not used) due to the resources created.

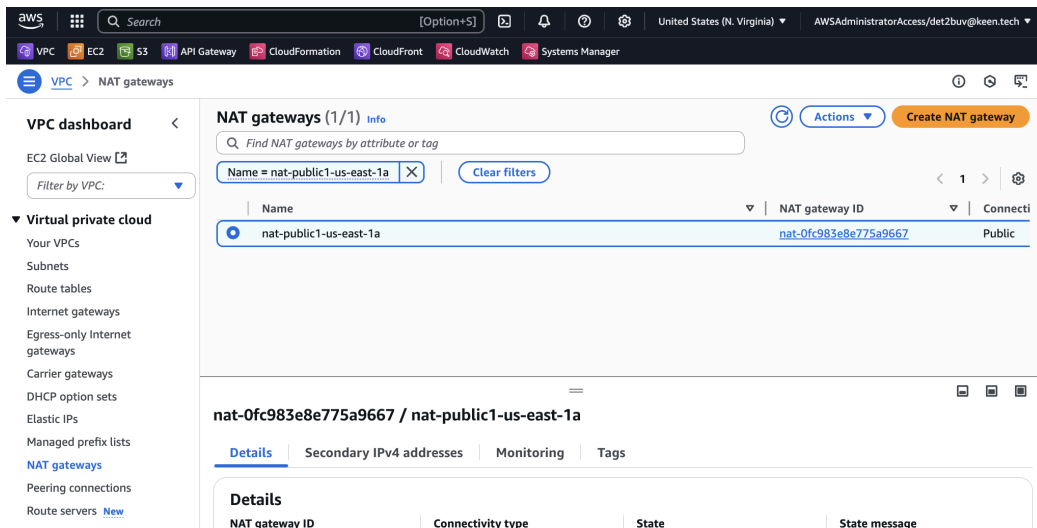
Deleting your VPC

To delete all resources perform the following steps:

1. Log in to the AWS Management Console.
2. Navigate to the VPC service and the planned region

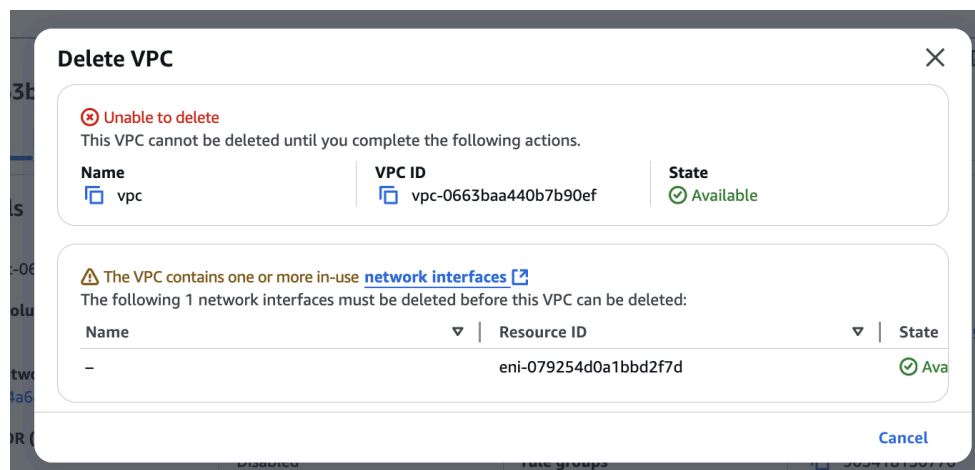


3. Select the NAT Gateway service, locate the NAT gateway created and press action → delete NAT gateway



4. Wait for the NAT gateway to be deleted. This will take around 3 minutes.
5. Select the VPC service, locate the VPC created and select actions → Delete VPC.

A screen might pop-up which says "unable-to-delete", delete any resources indicated here manually before retrying the delete operation.



(Optional) Amazon SES

Amazon Simple Email Service (SES) provides a reliable, cost-effective email solution that will enhance the user experience of the RVOC Engine with critical notification capabilities:

1. System Notifications

- Alert administrators about intercom system status changes

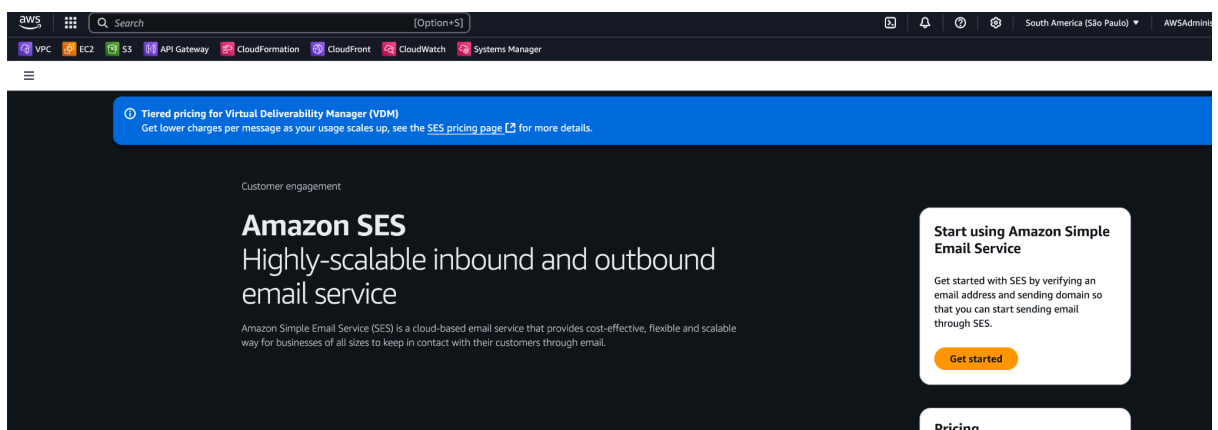
2. User Management

- Send welcome emails during user onboarding
- Send password reset notifications

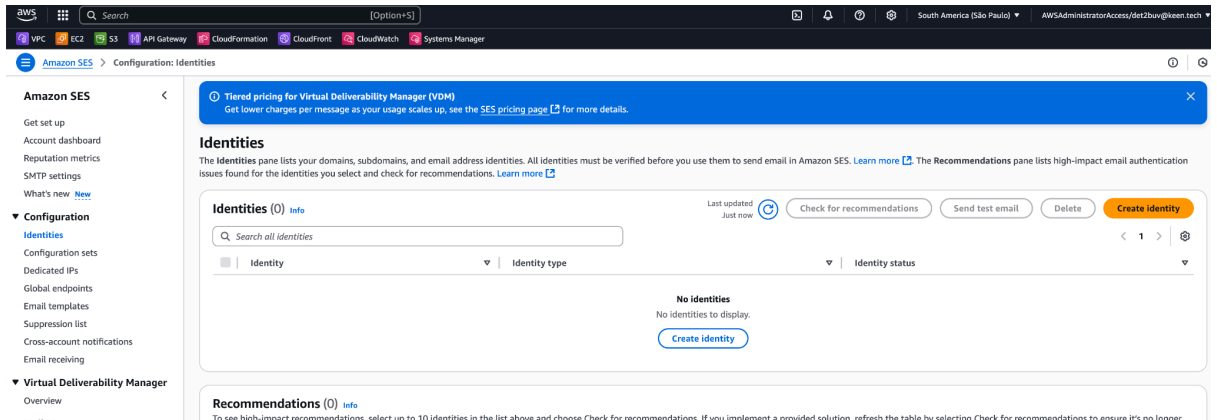
In this manual we will show how to setup Amazon SES with Domain ownership through Route53. Other configurations are possible, please see the Amazon SES documentation for other options.

Setting Up Amazon SES with Domain Authentication

1. Navigate to the Amazon Simple Email Service in the region in which you will deploy the intercom

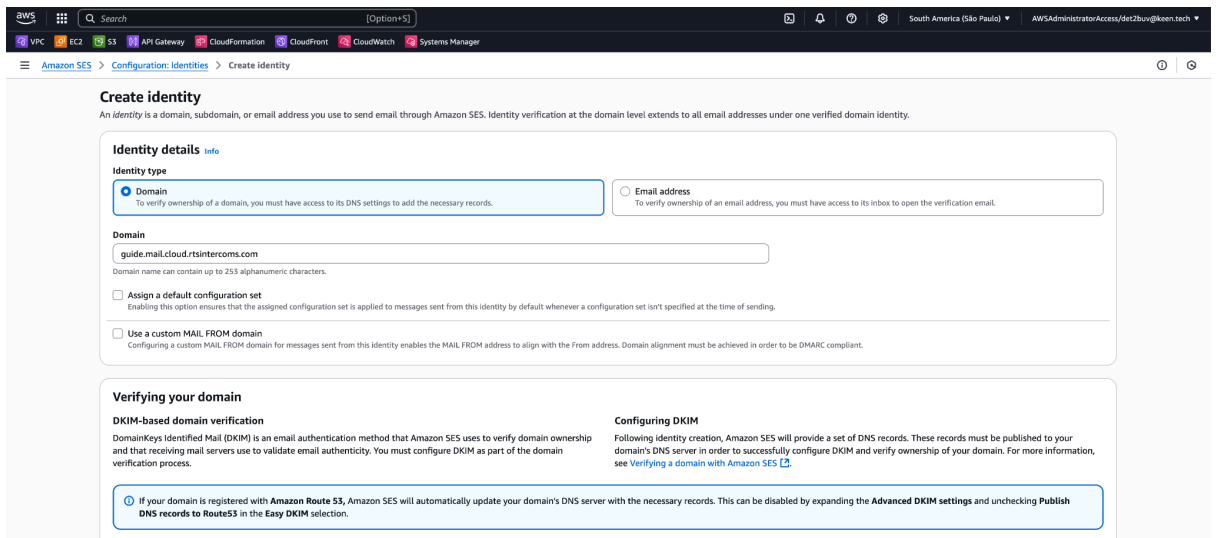


2. Press the “Menu icon” on the right to side, and navigate to Configuration Identities



3. Press “Create Identity”
4. Ensure to select “Domain” and provide the domain you want to use to send emails from.

In this example, we configure SES to send emails from “something”@[guide.mail.cloud.rtsintercoms.com](mailto:something@guide.mail.cloud.rtsintercoms.com), in the same AWS account a Route53 hosted zone exists for mail.cloud.rtsintercoms.com



5. Scroll down, ensure easy DKIM is selected, use all default settings as below:

Verifying your domain

DKIM-based domain verification

DomainKeys Identified Mail (DKIM) is an email authentication method that Amazon SES uses to verify domain ownership and that receiving mail servers use to validate email authenticity. You must configure DKIM as part of the domain verification process.

Configuring DKIM

Following identity creation, Amazon SES will provide a set of DNS records. These records must be published to your domain's DNS server in order to successfully configure DKIM and verify ownership of your domain. For more information, see [Verifying a domain with Amazon SES](#).

If your domain is registered with Amazon Route 53, Amazon SES will automatically update your domain's DNS server with the necessary records. This can be disabled by expanding the **Advanced DKIM settings** and unchecking **Publish DNS records to Route53** in the **Easy DKIM** selection.

Advanced DKIM settings

Identity type

☒ Easy DKIM

To set up Easy DKIM, you have to modify the DNS settings for your domain.

☐ Deterministic Easy DKIM

Utilize the Easy DKIM setup from a parent region and sign the new identity without additional DNS setup.

☐ Provide DKIM authentication token (BYODKIM)

Configure DKIM for this domain by providing your own private key.

DKIM signing key length

Signing key length is bits required in sign-in algorithm. DKIM 2048 is the recommended way to enhance security.

☒ RSA_2048_BIT

☐ RSA_1024_BIT

Publish DNS records to Route53

Amazon SES will automatically publish the required CNAME records to your domain's DNS settings in Route53 if your domain is registered.

☒ Enabled

DKIM signatures

DKIM signatures help validate that a message was not forged or altered in transit. Disabling this feature is not recommended.

☒ Enabled

6. Press "Create identity"
7. Amazon SES automatically creates the required DNS entries in Route53.

Validate whether the entries are created by Navigating to Route53, opening the hosted zone which is registered, look for "domainkey". Amazon SES should have created at least 3 entries:

Public mail.cloud.rtsintercoms.com Info

Hosted zone details

Records (5) DNSSEC signing Hosted zone tags (0)

Records (5) Info

Automatic mode is the current search behavior optimized for best filter results. [To change modes go to settings.](#)

Filter records by property or value

3 matches

Type Routing p... Alias 3 matches

domainkey X Clear filters

<input type="checkbox"/>	Record name	Type	Routing...	Differ...	Alias	Value/Route traffic to	TTL (s...	Health
<input type="checkbox"/>	cmstzicmycrafvgffepn7y7v6uukqpc_domainkey.guide.mail.cloud.rtsintercoms.com	CNAME	Simple	-	No	cmstzicmycrafvgffepn7y7v...	1800	-
<input type="checkbox"/>	gx6ntfni3hbh6aq2ipqxcubyo4cszma_domainkey.guide.mail.cloud.rtsintercoms.com	CNAME	Simple	-	No	gx6ntfni3hbh6aq2ipqxcubyo...	1800	-
<input type="checkbox"/>	swjjs6skzlsrdh5ige2rafsappvej_domainkey.guide.mail.cloud.rtsintercoms.com	CNAME	Simple	-	No	swjjs6skzlsrdh5ige2rafsapp...	1800	-

8. Amazon SES will now show the created identity as "Verification Pending", wait until the Identity Status moves to Verified. This can take up to 2 hours. In case the identity does not go to "Verified", contact your cloud administrator or AWS Support.

Identities

The Identities pane lists your domains, subdomains, and email address identities. All identities must be verified before you use them to send email in Amazon SES. [Learn more](#). The Recommendations pane lists high-impact email authentication issues found for the identities you select and check for recommendations. [Learn more](#)

Identities (1) Info

Last updated Just now

Check for recommendations Send test email Delete Create identity

Search all identities

< 1 > ⚙

<input type="checkbox"/>	Identity	Identity type	Identity status
<input type="checkbox"/>	guide.mail.cloud.rtsintercoms.com	Domain	Verification pending

9. Amazon SES initially places all new accounts in a "sandbox" environment with significant limitations. Once your domain is verified you must

request production access.

Navigate to SES console → 'Account dashboard' → 'Production Access'

10. Complete the request form with:

- Select: Transactional
- Reason: We have installed RVOC Engine (see <https://rtsintercoms.com/rvoc>). RVOC Engine uses Amazon SES to send invitation emails to users which are added through a manual sign-up process as well as password reset request.

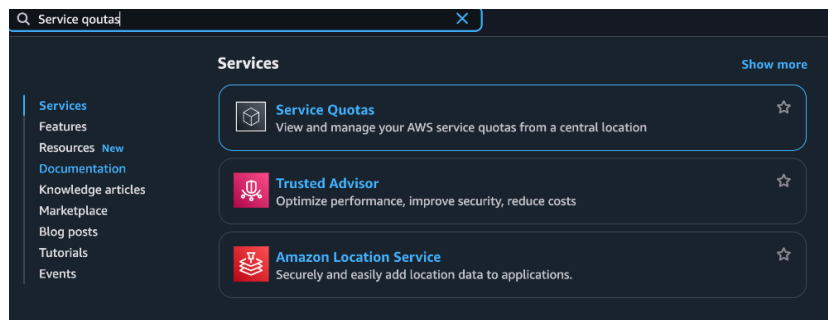
11. Production approval typically processes within 24-48 hours.

Amazon EC2 - Elastic IP

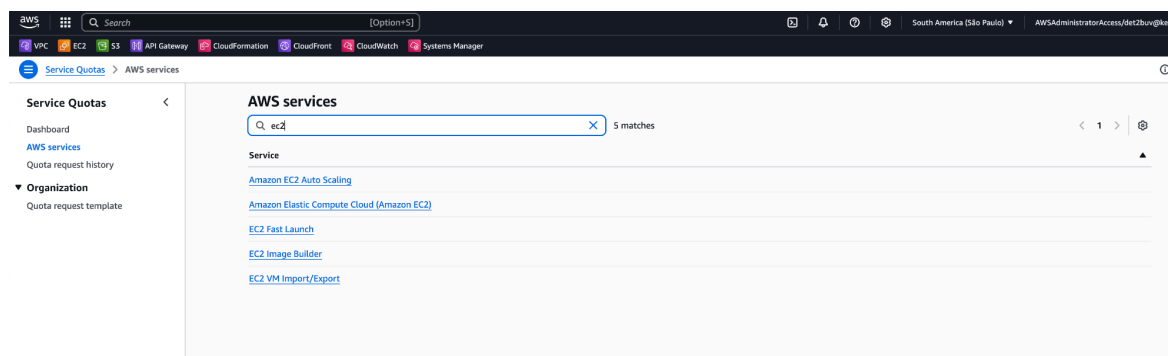
A standard deployment requires 2 public IP addresses (1 for Intercom, 1 for Turn server), a high-available deployment requires 4 addresses (2 for Intercom, 2 for Turn Server, 2 for Global Accelerator). Additional Elastic IP addresses are required for your VPC Setup (1 IP for a single AZ VPC, at least 2 IP's for a multi AZ VPC).

Note that by default only 5 elastic IP's are available per AWS account / region, additional Elastic IP's require a service quota increase

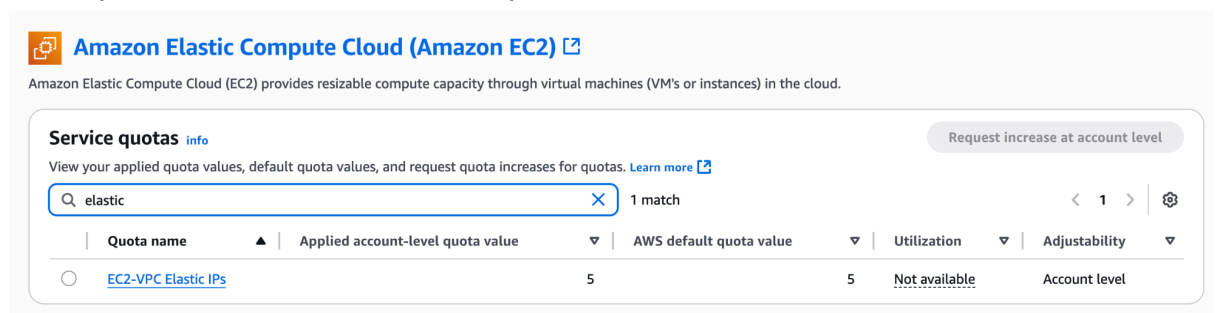
1. Navigate to the "Service Quota" service **in the region** in which you require the additional addresses.



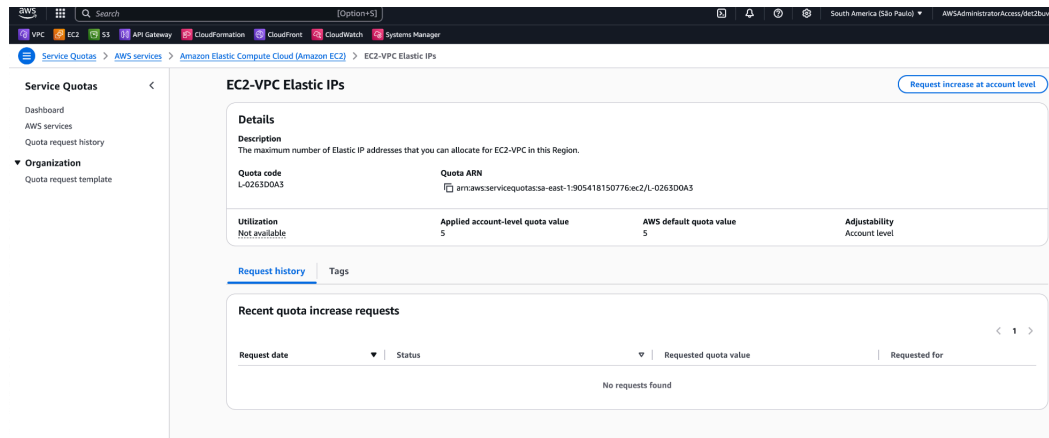
2. Search to the Amazon Elastic Compute Cloud (Amazon EC2) Service and select it



3. Lookup the EC2-VPC Elastic IPs quota:



4. Select the quota and request an increase at account level. A typical good number to request for RVOC high availability deployments is 10 (including your NAT gateway IP's)



5. Depending on your level of support the service quota increase may take anywhere between 30 minutes and 2 days.

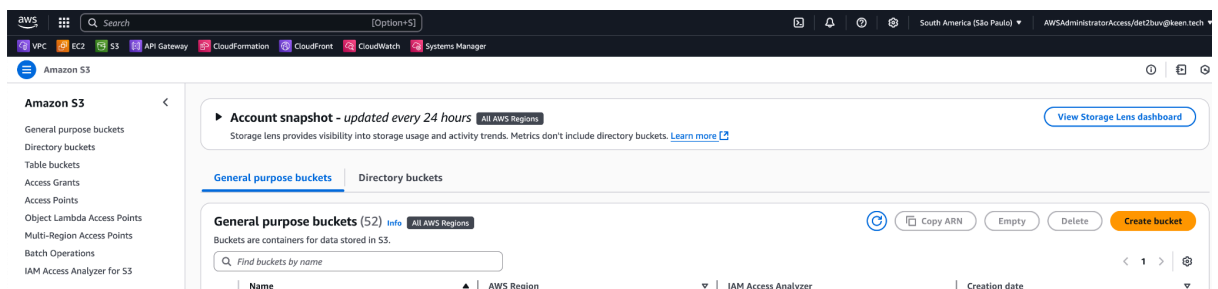
Amazon S3 Bucket

RVOC Engine requires a bucket to be created which hosts the RVOC engine software.

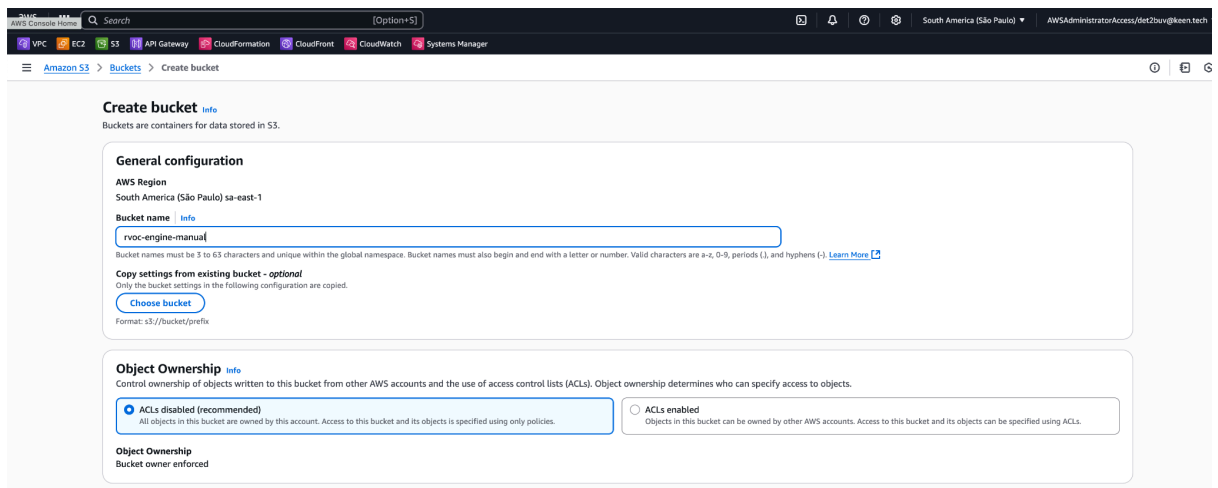
Note: Amazon S3 is a global service, to decrease latency it is advised to create the S3 bucket in the same region as you are planning to deploy the RVOC engine.

To create a bucket and upload the RVOC Engine software follow the following steps:

1. Select the region in which you are planning to deploy the RVOC Engine
2. Navigate to the Amazon S3 service
3. Press Create Bucket



4. Provide a name for the Amazon S3 bucket. The name has to be globally unique, note that creation will fail when the name is already in use.



5. Keep all settings default, scroll down and press "Create Bucket"

Frequently asked questions

1. How to calculate the expected data egress costs for my RVOC engine?

You can calculate the expected data egress costs in RVOC elevate. Note that this uses an estimation of the usages of the different ports.

RVOC engine uses different techniques to limit the bandwidth usage to the necessary usage. Enabling VAD on RVON connections will help here greatly.

2. Why does an RVOC engine require a public and private subnet?

RVOC Engine deployments try to comply with public best practices such as CIS Benchmark Guidelines for AWS VPC Subnet Architecture.

This recommends network segmentation for public and private resources, therefore the Intercom itself is placed in the private network later, while load balancers are used to disclose communication paths to the intercom?

3. How many private IP addresses does my RVOC engine use?

At a minimum the RVOC engine uses 4 private IP addresses in the public subnet, and 1 private IP address in the private subnet.

However;

- There are different deployment options which will increase the number of IP addresses in use
- Depending on the traffic, the load balancers might scale requiring additional IP addresses.

4. What is the effect of the use of AWS Global Accelerator on my latency?

Note that AWS Global Accelerator is only used for RVON connections.

AWS advertises that AWS Global Accelerator improves the network performance for up to 60%, the network improvement you will see will differ depending on your setup.

5. Why does RVOC engine require AWS global accelerator in case of High Availability.

AWS global accelerator provides a single global static IP to be used for RVON connections. Global accelerator will automatically route the traffic to the health and in use availability zone.

6. How many Elastic IP's does RVOC require?

A standard deployment requires 2 public IP addresses (1 for Intercom, 1 for Turn server), a high-available deployment requires 6 addresses (2 for Intercom, 2 for Turn Server, 2 for Global Accelerator).

Note that by default only 5 elastic IP's are available per AWS account / region, additional Elastic IP's require a service quota increase.

7. Why does SMTP over port 25 not work?

AWS does restrict the usage of port 25 by default:

<https://repost.aws/knowledge-center/ec2-port-25-throttle>

Move to a secure port or request AWS to remove the restriction.