SIEMENS

SIMATIC NET

Industrial Remote Communication - Remote Networks SINEMA RC Server in the cloud

Getting Started

03/2021
C79000-G8976-C640-01

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

C79000-G8976-C640-01
Ⓟ 03/2021 Subject to change

Table of contents

Preface 1

Purpose of this documentation

Example for connection of SINEMA RC Server in the cloud.

Validity of this documentation

This manual is valid for the following software version:

- SINEMA Remote Connect as of version V3.0

Current manuals and further information

You will find the current manuals and further information on remote networks products on the Internet pages of Siemens Industry Online Support:

- Using the search function:

  Link to Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/ps/21816)

  Enter the entry ID of the relevant manual as the search item.

- via the navigation in the "Remote Networks" area:

  Link to the "Remote Networks" area (https://support.industry.siemens.com/cs/ww/en/ps/21778)

  Go to the required product group and make the following settings:
  "Entry list" tab, Entry type "Manuals"

You will find the documentation for the products relevant here on the data storage medium that ships with some products:

- Product CD / product DVD
- SIMATIC NET Manual Collection

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines, and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions form one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. These systems, machines and components should only be connected to the enterprise network or the Internet if and only to the extent necessary and with appropriate security measures (firewalls and/or network segmentation) in place.

You can find more information on protective measures in the area of industrial security by visiting:
https://www.siemens.com/industrialsecurity (https://www.siemens.com/industrialsecurity).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends performing product updates as soon as they are available and using only the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under
https://www.siemens.com/industrialsecurity (https://www.siemens.com/industrialsecurity).

Introduction 2

In this example configuration, we show you how to migrate the SINEMA RC Server to Amazon S3 (Amazon Simple Storage Service).

To do so, the virtual machine is uploaded to the cloud. So that it is executable, the virtual machine is imported via the AWS CLI to an Amazon Machine Image (ami).

Requirements

- Install the SINEMA RC Server V3.0 in a virtual machine.
- For the installation, select the dynamic assignment of the IP address via DHCP, e.g., 192.168.9.90.
- Before the initial logon, export the virtual machine as an ova file. The ova file contains the files that are necessary for the virtual machine.

  If the virtual machine is uploaded to the cloud before the initial logon, a separate key and a separate certificate is created for each instance that is derived from the AMI.

IP settings

The IP settings used in the configuration example were freely chosen.

In a real network, you would need to adapt these IP settings to avoid possible address conflicts.

Additional information

- AWS documentation (https://docs.aws.amazon.com/index.html)

Amazon Cloud (AWS) 3

3.1 Uploading the ova file

For the virtual machine to be reachable in the cloud, the ova file is uploaded.

Requirement

- You have a valid AWS account.

Procedure

1. Log in to the AWS management console.
2. Click on "All services".
3. Under "Storage", click on "S3".
4. For uploading create an AWS bucket in an AWS region. Click on "Create bucket".

   Enter the name "sinema-remote-connect".

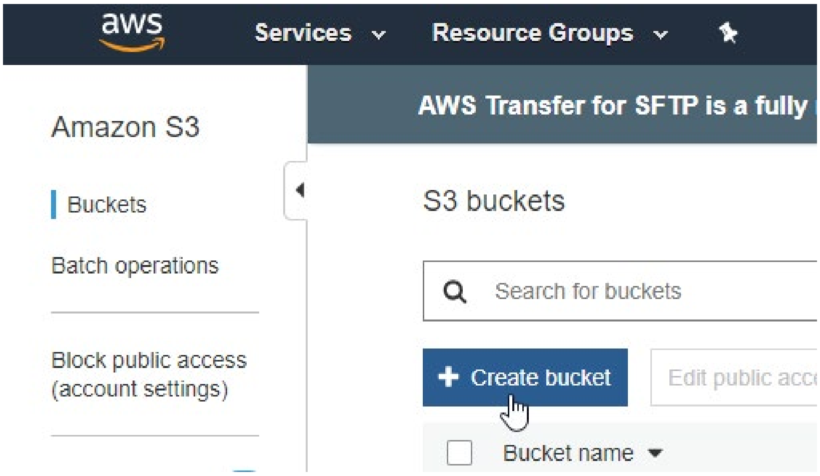


Figure 3-1 Bucket

The AWS region must correspond to the region in which the SINEMA RC Server is to be located, for example, Europe (Frankfurt) - eu-central-1.

To upload the ova file, click on "Upload" and select the ova file.

3.2 Importing ova in AMI

3.2.1 Configuring AWS CLI

To configure the AWS CLI, you need an "Access Key ID" and an associated "Secret Access Key". This access information is assigned when the user is created.

Requirement

- You have a valid AWS account.

Procedure

1. Log in to the AWS management console. Under "Security, Identity & Compliance", click on "IAM".
2. The "Identity & Access Management (IAM)" opens. Under "Access Management", click on "Users".
3. Click on "Add User". Enter a user name, for example, SRCAdmin.

   For "Access type", select "Programmatic access" and click on "Next: Permission".
4. In this example the user is assigned the "AdministratorAccess" policy.

   Click on "Attach existing policies directly" and select "AdministratorAccess".
5. Click on "Next: Tags" and "Next: Preview".
6. To create the user, click on "Create User".

   The access key is generated. Download the download.csv file. This file contains the Access Key ID and the Secret Access Key.

   This information is only displayed in this window and cannot be retrieved again later.
7. Install the AWS CLI.
8. To configure the AWS CLI, you need the "Access Key ID" and the associated "Secret Access Key".
9. Open the Command Prompt on the PC.
10. Configure the AWS CLI.

    Example

    ```
    > aws configure
       AWS Access Key ID [None]: AKIxxxxxxxxxxxJXR7A
       AWS Secret Access Key [None]:
    q3YKo+xxxxxxxxxxxxxxxxxxxxnj0nDkGy4l
       Default region name [None]: eu-central-1
       Default output format [None]: json
    ```

Additional information

AWS documentation "Installing AWS CLI (https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-install.html)"

AWS documentation "Configuring AWS CLI (https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-configure.html)"

3.2.2 Importing virtual machine as AMI

Requirement

- You have a valid AWS account.

Configuring the IAM role "vmimport"

The import requires a role to execute the operation.

1. Create the `trust-policy.json` file and save it.

   Example:

   ```
   {
      "Version": "2012-10-17",
      "Statement": [
         {
            "Effect": "Allow",
            "Principal": { "Service": "vmie.amazonaws.com" },
            "Action": "sts:AssumeRole",
            "Condition": {
               "StringEquals":{
                  "sts:Externalid": "vmimport"
               }
            }
         }
      ]
   }
   ```

2. Open the Command Prompt on the PC.
3. You create the role with the command:

   Example

   ```
   > aws iam create-role --role-name vmimport --assume-role-policy-
   document "file://C:\import\trust-policy.json"
   ```

   For `file` enter the complete path to the storage location of the file.

4. Create a file with the name `role-policy.json` to assign the corresponding policies for the import to the IAM role.

   Example:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect": "Allow",
         "Action": [
            "s3:GetBucketLocation",
            "s3:GetObject",
            "s3:ListBucket"
         ],
         "Resource": [
            "arn:aws:s3:::sinema-remote-connect",   Bucket for data
storage medium image (Page 9)
            "arn:aws:s3:::sinema-remote-connect/*"
         ]
      },
      {
         "Effect": "Allow",
         "Action": [
            "s3:GetBucketLocation",
            "s3:GetObject",
            "s3:ListBucket",
            "s3:PutObject",
            "s3:GetBucketAcl"
         ],
         "Resource": [
            "arn:aws:s3:::sinema-remote-connect", Bucket for exported
images (Page 9)
            "arn:aws:s3:::sinema-remote-connect/*"
         ]
      },
      {
         "Effect": "Allow",
         "Action": [
            "ec2:ModifySnapshotAttribute",
            "ec2:CopySnapshot",
            "ec2:RegisterImage",
            "ec2:Describe*"
         ],
         "Resource": "*"
      }
   ]
}
```

5. You assign the policy to the role with the command:

   Example

   ```
   > aws iam put-role-policy --role-name vmimport --policy-name
   vmimport --policy-document "file://C:\import\role-policy.json"
   ```

   For `file` enter the complete path to the storage location of the file.

Additional information

- AWS documentation "VM Import/Export" in the section "Required service role (https://docs.aws.amazon.com/vm-import/latest/userguide/vmie_prereqs.html#vmimport-role)"

Importing the ova file in AMI

1. Create the `container.json` file and save it.

   Example:

   ```
   [
     {
       "Description": "SINEMA RC V3.0",
       "Format": "ova",
       "UserBucket": {
           "S3Bucket": "sinema-remote-connect",
           "S3Key": "SinemaRC.ova"
       }
   }]
   ```

2. You start the import with the command.
3. Example

   ```
   > aws ec2 import-image --description "SINEMA RC V3.0" --disk-
   containers "file://C:\import\container.json"
   ```

   For `file` enter the complete path to the storage location of the file.

Additional information

- AWS documentation "VM Import/Export" in the section "Importing a VM as an image using VM Import/Export (https://docs.aws.amazon.com/vm-import/latest/userguide/vmimport-image-import.html)".

3.3 Configuring basic data

3.3.1 Creating a VPC

To operate the SINEMA RC application in a secure environment, you create an Amazon Virtual Private Cloud (VPC).

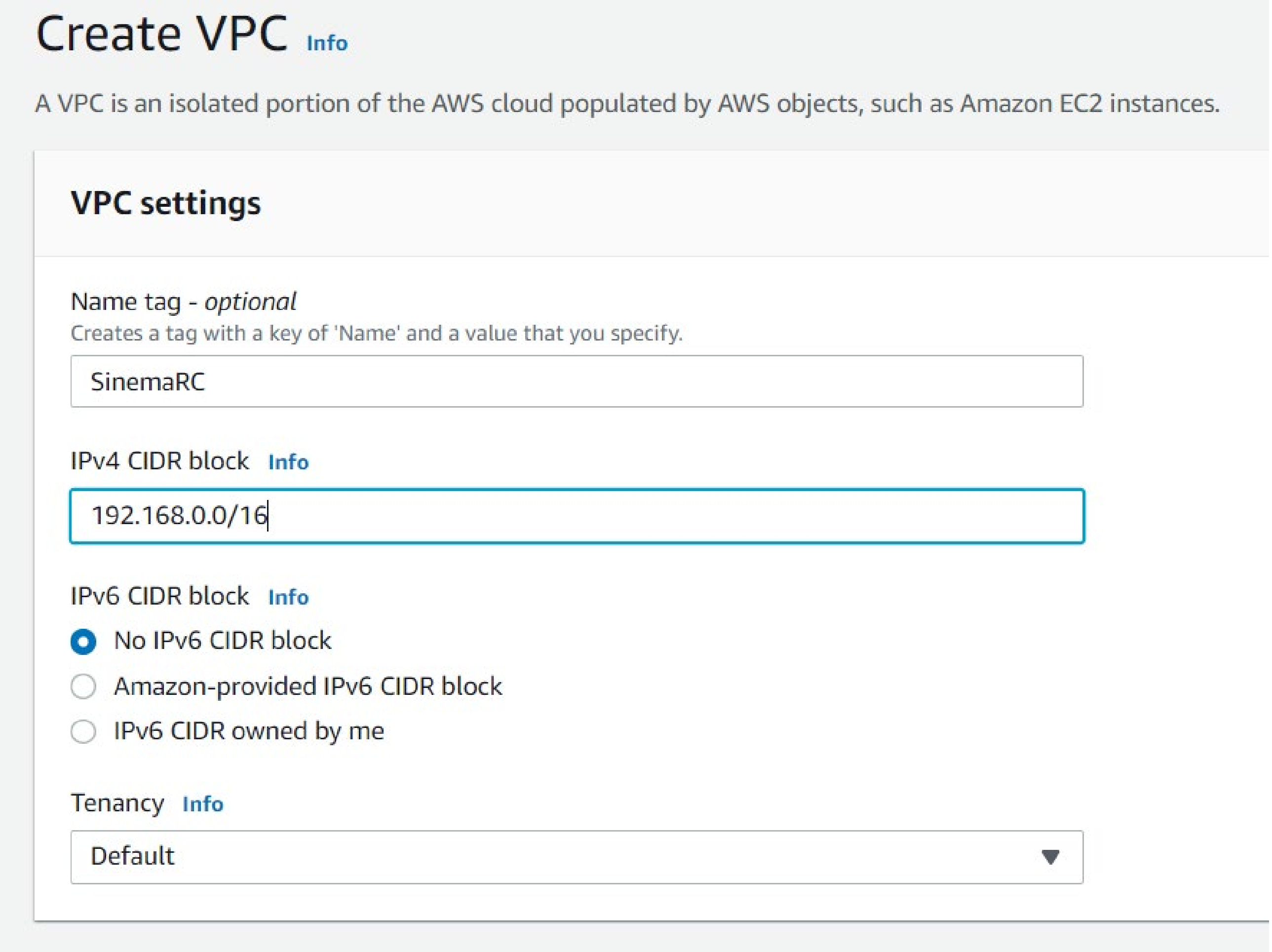
Requirement

- You have a valid AWS account, and you are logged in to the AWS management console.

Procedure

1. For "Networking & Content Delivery", click on "My VPC" (Virtual Private Cloud).
2. Click on "Create VPC".
3. Enter the name "sinemarc".

4. Enter an "IPv4 CIDR block" that matches the settings of the SINEMA RC server.



Create VPC Info

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.
SinemaRC

IPv4 CIDR block Info
192.168.0.0/16

IPv6 CIDR block Info
● No IPv6 CIDR block
○ Amazon-provided IPv6 CIDR block
○ IPv6 CIDR owned by me

Tenancy Info
Default ▼

5. Click on "Create VPC". The VPC "sinemarc" is listed in the overview.

Additional information

AWS documentation "Amazon VPC" in the section "VPCs and subnets (https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Subnets.html)".

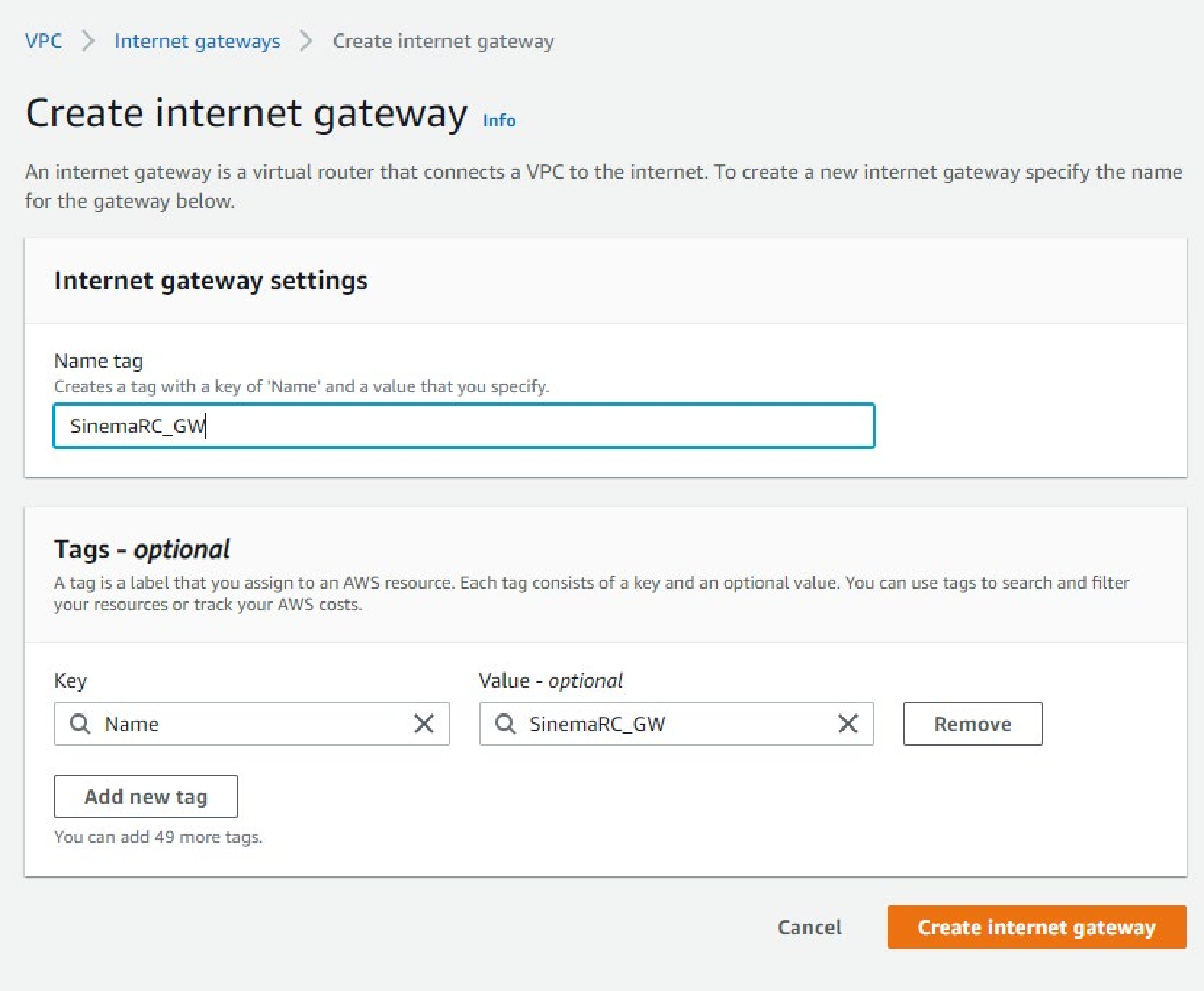
3.3.2 Adding an internet gateway to the VPC

Requirement

- You have a valid AWS account, and you are logged in to the AWS management console.
- VPC dashboard is open.

Adding an internet gateway

1. Under "Virtual Private Cloud", click on "Internet Gateway".
2. Click on "Create internet gateway".



VPC > Internet gateways > Create internet gateway

Create internet gateway Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag
Creates a tag with a key of 'Name' and a value that you specify.
SinemaRC_GW

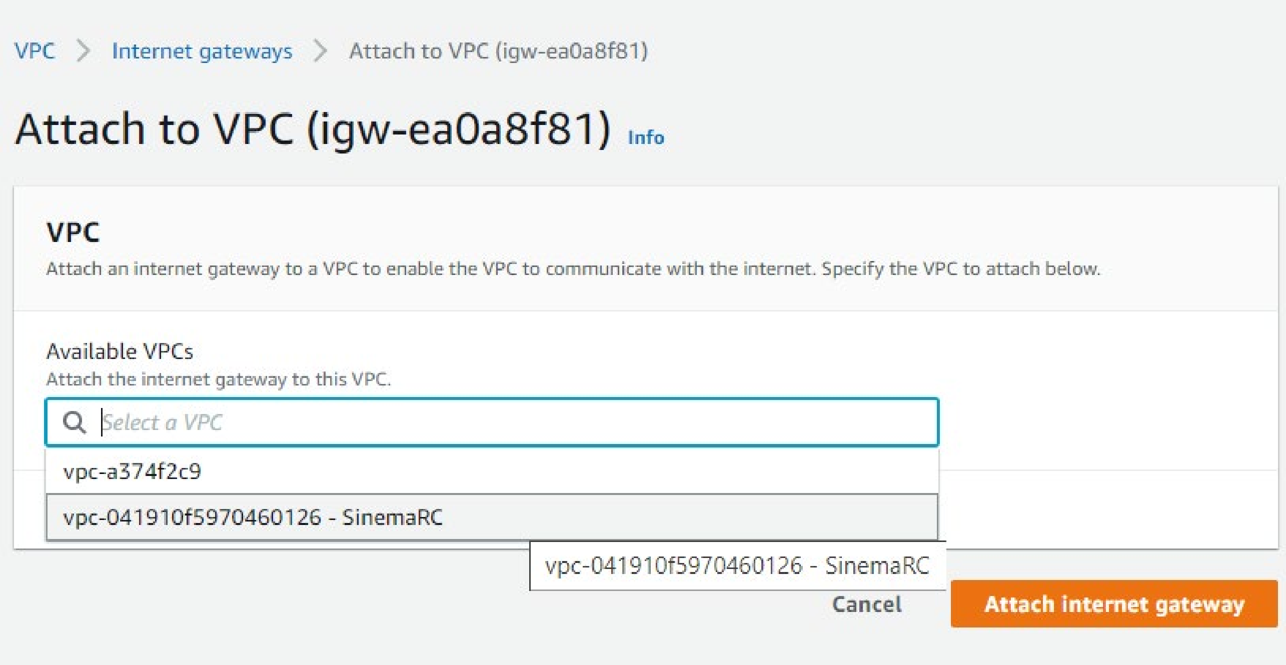
Tags - *optional*
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*	
Name	SinemaRC_GW	Remove

Add new tag
You can add 49 more tags.

3. Enter a name and click on "Create internet gateway".
4. Right-click on the name of the internet gateway.

5. Select "Attach to VPC".



VPC > Internet gateways > Attach to VPC (igw-ea0a8f81)

Attach to VPC (igw-ea0a8f81) Info

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

Select a VPC

vpc-a374f2c9

vpc-041910f5970460126 - SinemaRC

vpc-041910f5970460126 - SinemaRC

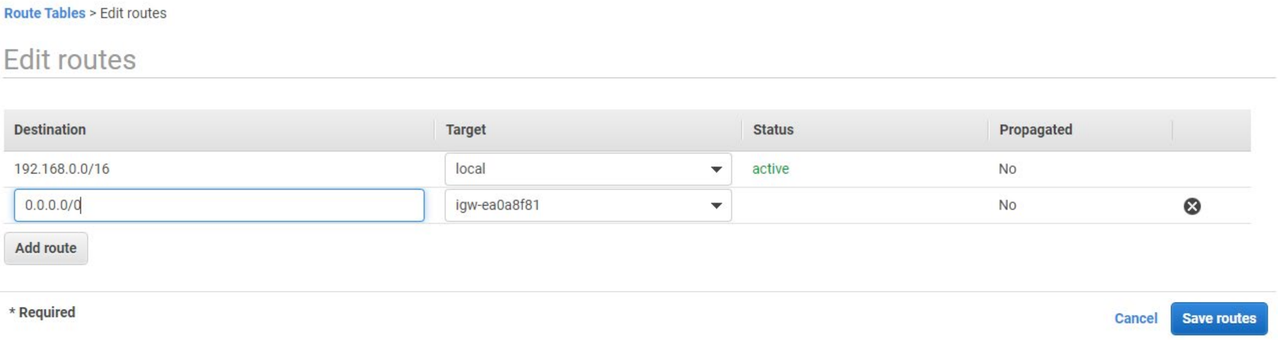
6. For "Available VPC", select "SinemaRC".
7. Click on "Attach internet gateway".

Adding a route

A route is added for access from the external network.

1. Under "Virtual Private Cloud", click on "Route Tables".
2. Right-click on the VPC name.
3. Select "Edit routes".

   For "Destination" enter "0.0.0.0/0" (all IP addresses) and for "Target" select the ID of the internet gateway.



Route Tables > Edit routes

Edit routes

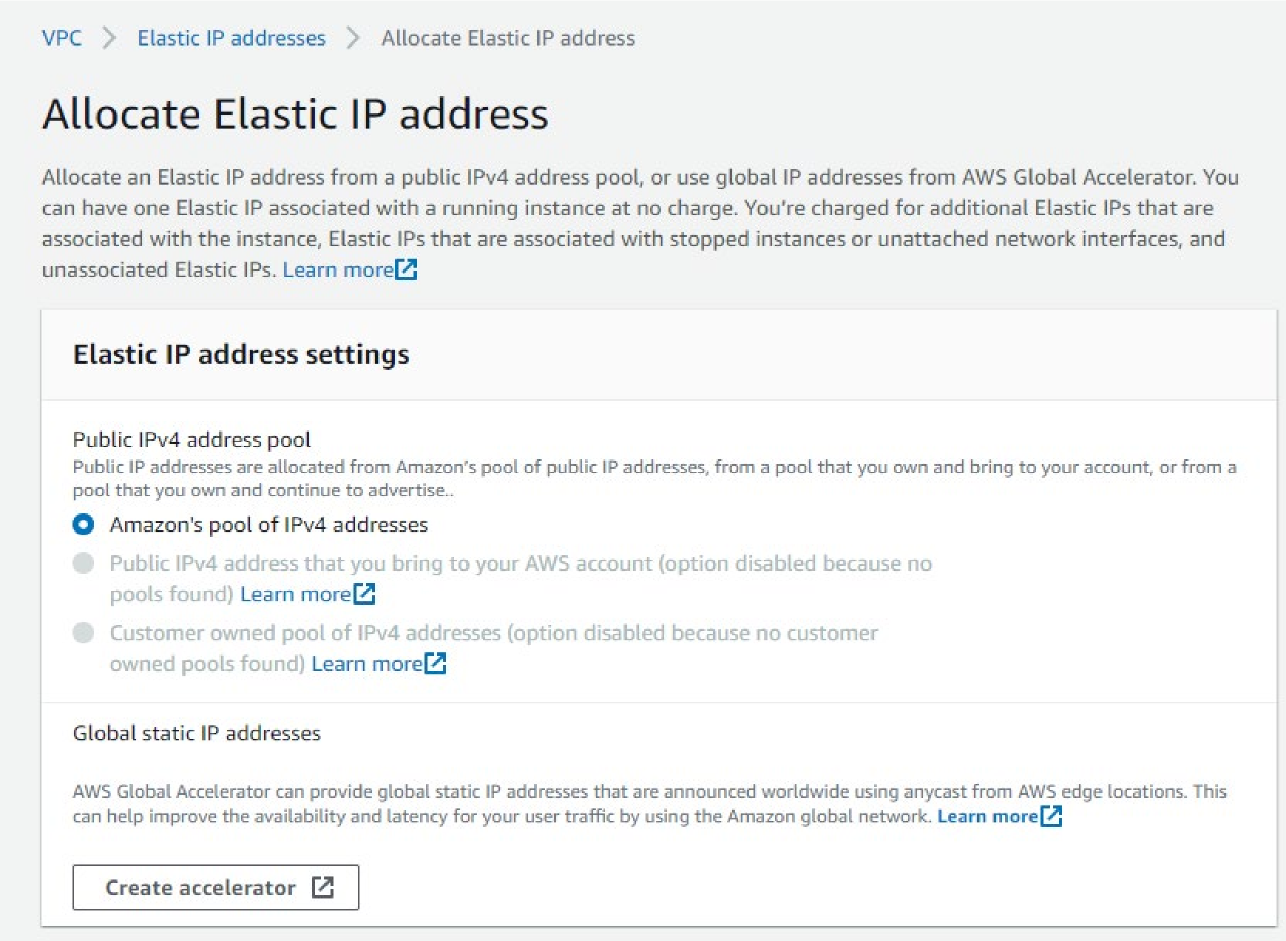
Destination	Target	Status	Propagated
192.168.0.0/16	local	active	No
0.0.0.0/0	igw-ea0a8f81		No

4. Click on "Save routes".

Adding an Elastic IP address

The SINEMA RC Server can be reached via the internet using the Elastic IP address.

1. Under "Virtual Private Cloud", click on "Elastic IPs".
2. Click on "Allocate Elastic IP address".



Allocate Elastic IP address

Allocate an Elastic IP address from a public IPv4 address pool, or use global IP addresses from AWS Global Accelerator. You can have one Elastic IP associated with a running instance at no charge. You're charged for additional Elastic IPs that are associated with the instance, Elastic IPs that are associated with stopped instances or unattached network interfaces, and unassociated Elastic IPs. Learn more

Elastic IP address settings

Public IPv4 address pool
Public IP addresses are allocated from Amazon's pool of public IP addresses, from a pool that you own and bring to your account, or from a pool that you own and continue to advertise..

- ● Amazon's pool of IPv4 addresses
- ○ Public IPv4 address that you bring to your AWS account (option disabled because no pools found) Learn more
- ○ Customer owned pool of IPv4 addresses (option disabled because no customer owned pools found) Learn more

Global static IP addresses

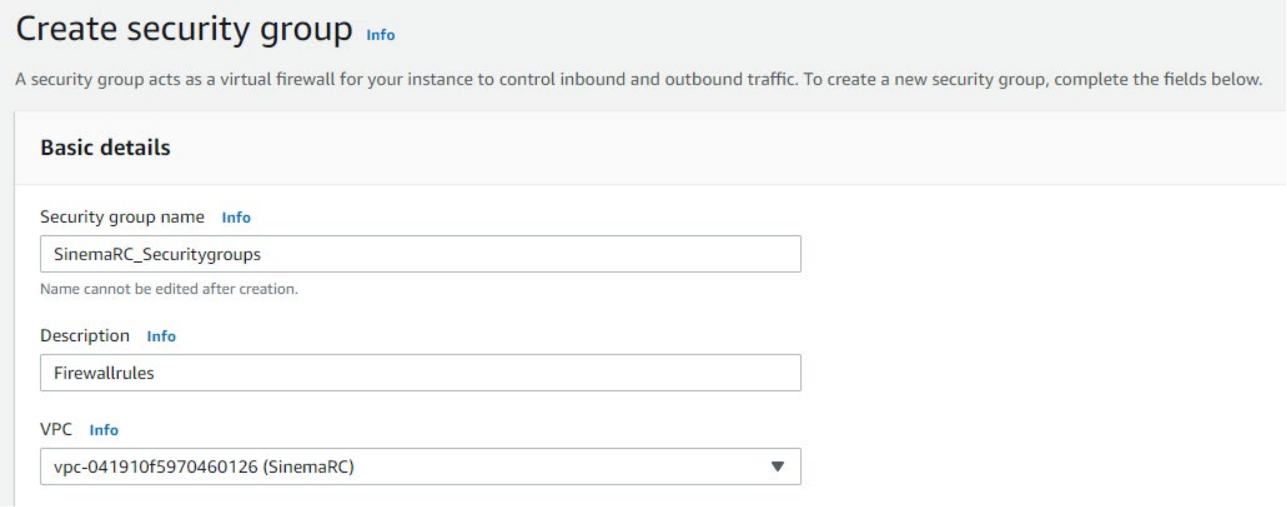
AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. Learn more

3. Use the default settings and click on "Allocate".

Creating a security group for internet access

1. Under "Security", click on "Security groups".
2. Click on "Create security group".

3. Enter a name and select "sinemarc" for "VPC".



Create security group

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name: SinemaRC_Securitygroups

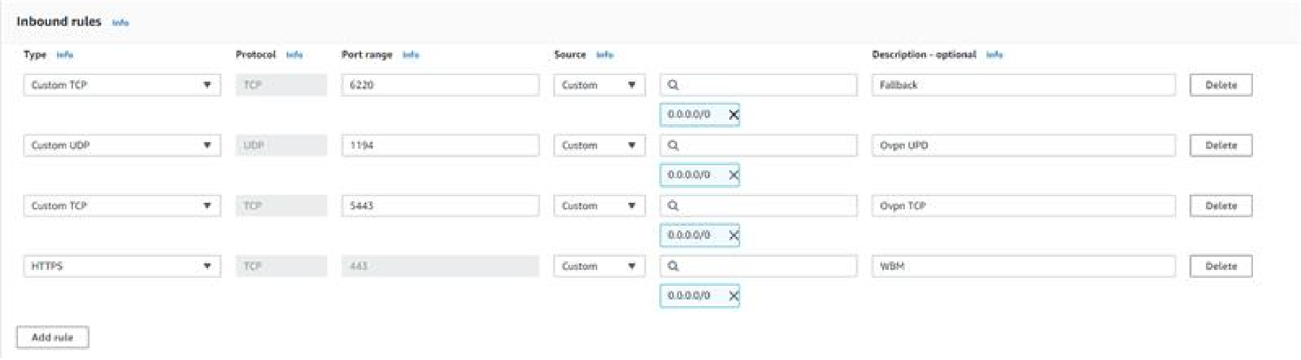
Name cannot be edited after creation.

Description: Firewallrules

VPC: vpc-041910f5970460126 (SinemaRC)

4. Configure the ports for inbound rules as follows:

Type	Protocol	Port range	Source	IP
Custom TCP	TCP	6220	Custom	0.0.0.0/0 All IP addresses
Custom UDP	UDP	1194	Custom	0.0.0.0/0 All IP addresses
Custom TCP	TCP	5443	Custom	0.0.0.0/0 All IP addresses
HTTPS	TCP	443	Custom	0.0.0.0/0 All IP addresses

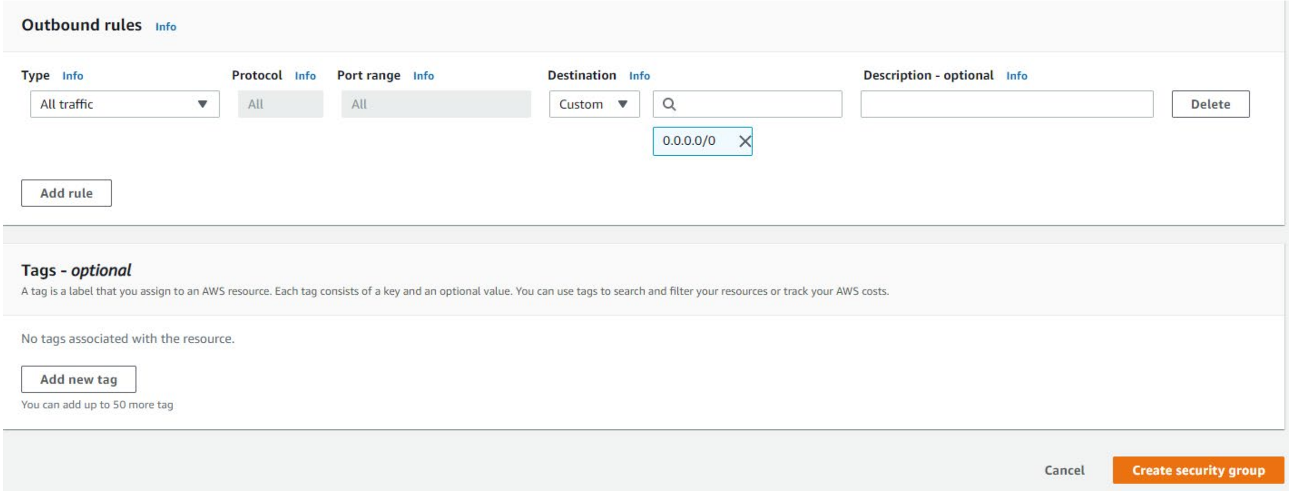


Inbound rules

Type	Protocol	Port range	Source		Description - optional
Custom TCP	TCP	6220	Custom	0.0.0.0/0	Fallback
Custom UDP	UDP	1194	Custom	0.0.0.0/0	Ovpn UPD
Custom TCP	TCP	5443	Custom	0.0.0.0/0	Ovpn TCP
HTTPS	TCP	443	Custom	0.0.0.0/0	WBM

5. Configure the ports for outbound rules as follows:

Type	Protocol	Port range	Source	IP
All traffic	All	All	Custom	0.0.0.0/0 All IP addresses



Outbound rules Info

Type: All traffic
Protocol: All
Port range: All
Destination: Custom
0.0.0.0/0
Description - optional

Tags - *optional*

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

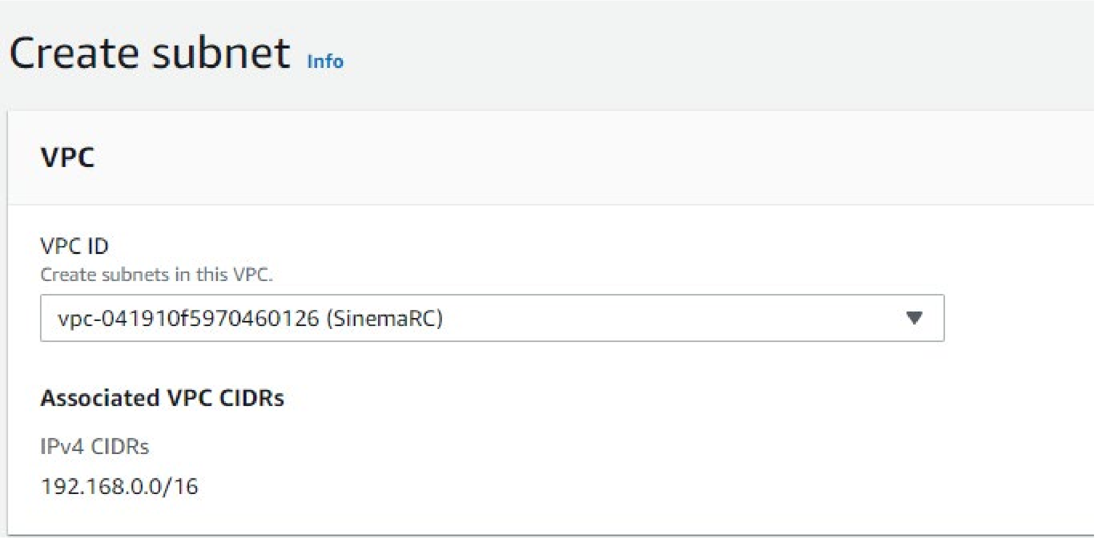
No tags associated with the resource.

You can add up to 50 more tag

6. Click on "Create security group".

Creating a subnet

1. Under "Virtual Private Cloud", click on "Subnets".
2. Click on "Create subnet" and select "sinemarc" for "VPC".



Create subnet Info

VPC

VPC ID
Create subnets in this VPC.
vpc-041910f5970460126 (SinemaRC)

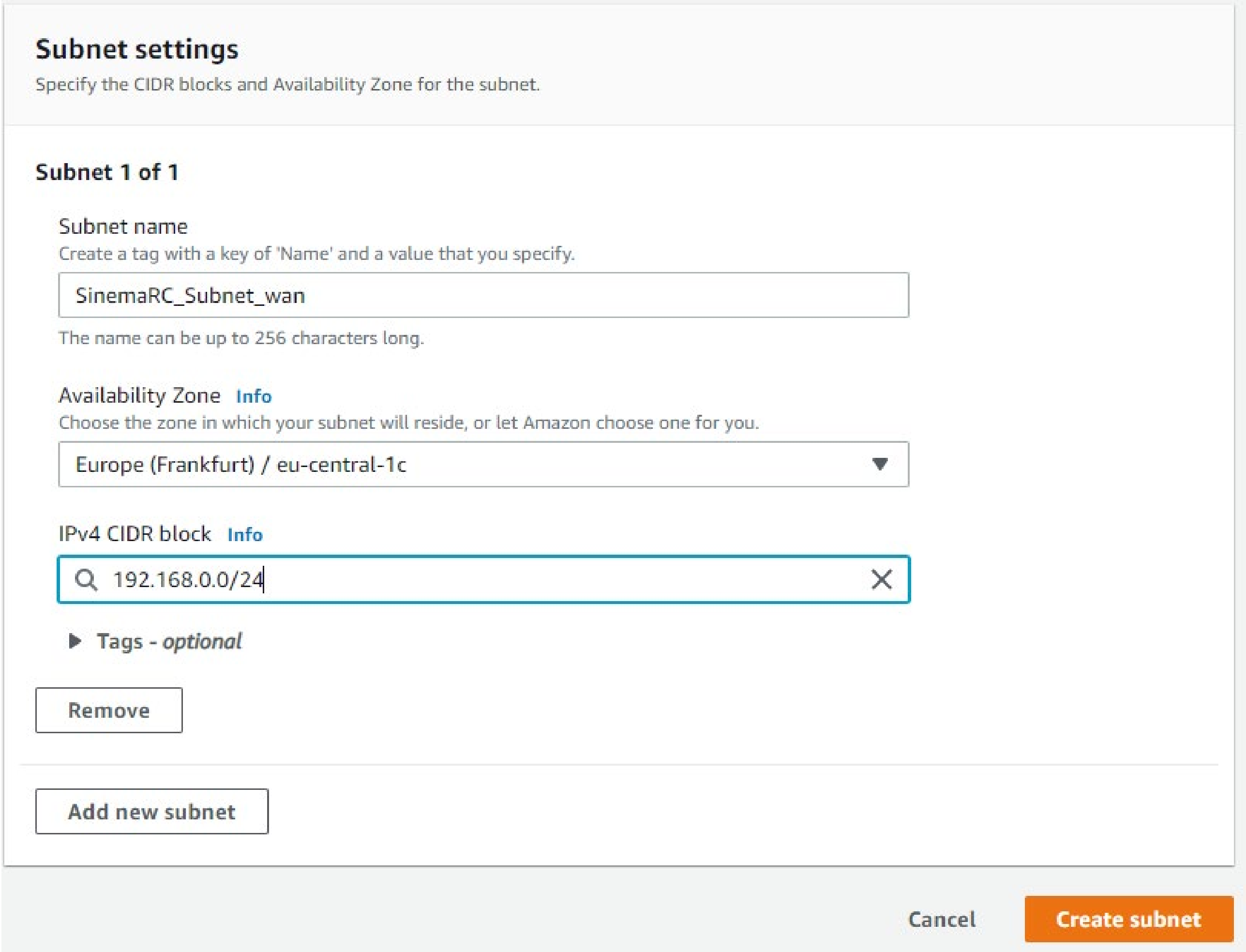
Associated VPC CIDRs

IPv4 CIDRs
192.168.0.0/16

You configure the subnet in the "Subnet settings" area.

3. Enter a name.
4. Do not change the setting for "Availability Zone".

5. Enter an IPv4 CIDR block that matches the settings of the SINEMA RC server.



Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

SinemaRC_Subnet_wan

The name can be up to 256 characters long.

Availability Zone Info

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

Europe (Frankfurt) / eu-central-1c

IPv4 CIDR block Info

192.168.0.0/24

6. Click on "Create subnet".

Additional information

AWS documentation "Amazon VPC" in the section "Adding an internet gateway to your VPC".

See also

Internet Gateway
(https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html)

3.3.3 Configuring the network interface

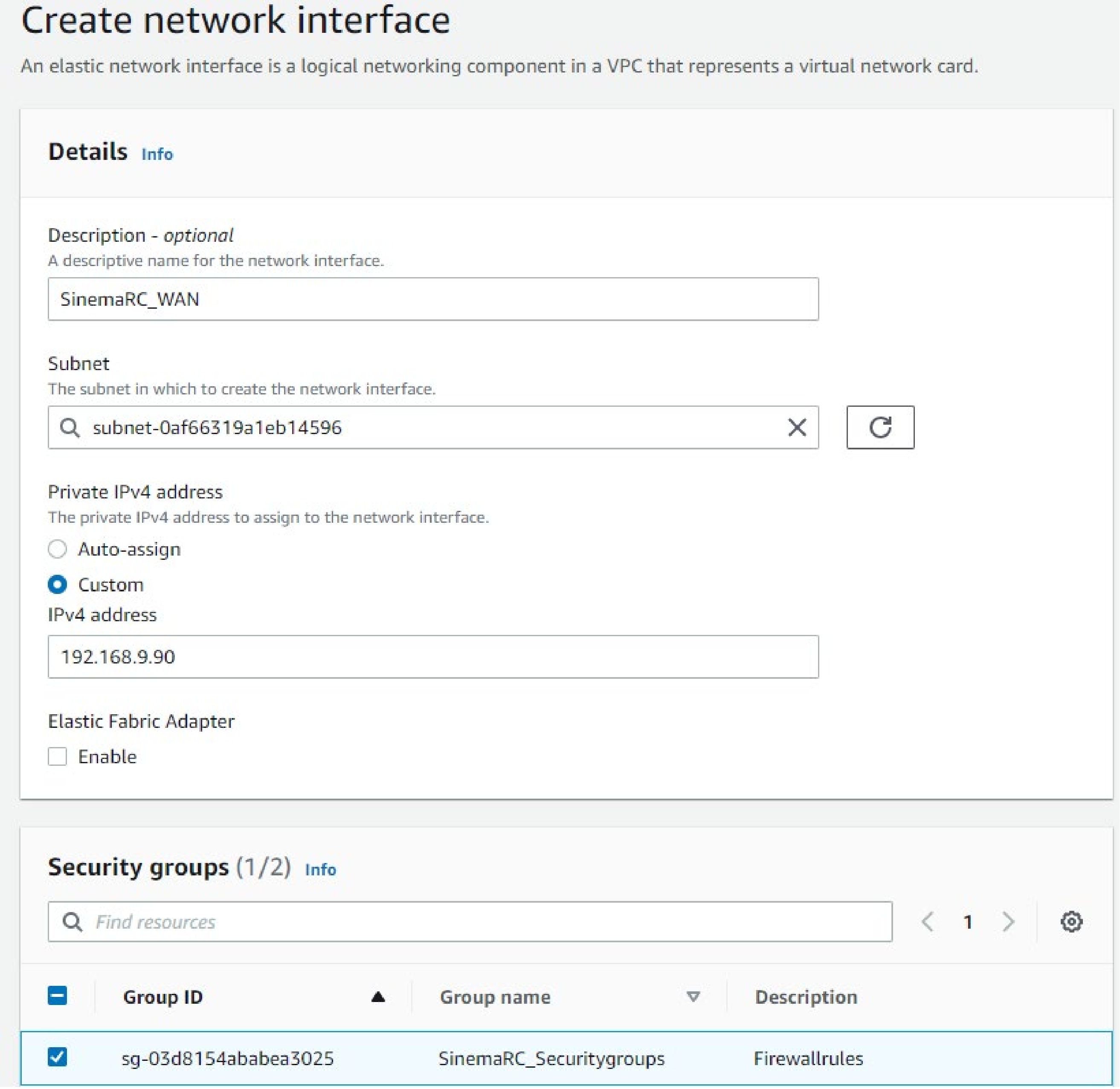
Requirement

- You have a valid AWS account, and you are logged in to the AWS management console.

Adding a network interface

1. For "Compute", click on "EC2". The EC2 dashboard opens.
2. For "Network & Security", click on "Network Interfaces".
3. Click on "Create Network Interface".
4. For "Subnet" select the subnet of the WAN interface.
5. For "Private IPv4 address" select "Custom" and enter the IP address (192.168.9.90) of the WAN interface for "IPv4 address".

6. For "Security groups" enable the configured security group.



Create network interface

An elastic network interface is a logical networking component in a VPC that represents a virtual network card.

Details Info

Description - *optional*
A descriptive name for the network interface.
SinemaRC_WAN

Subnet
The subnet in which to create the network interface.
subnet-0af66319a1eb14596

Private IPv4 address
The private IPv4 address to assign to the network interface.
○ Auto-assign
● Custom
IPv4 address
192.168.9.90

Elastic Fabric Adapter
□ Enable

Security groups (1/2) Info

Find resources

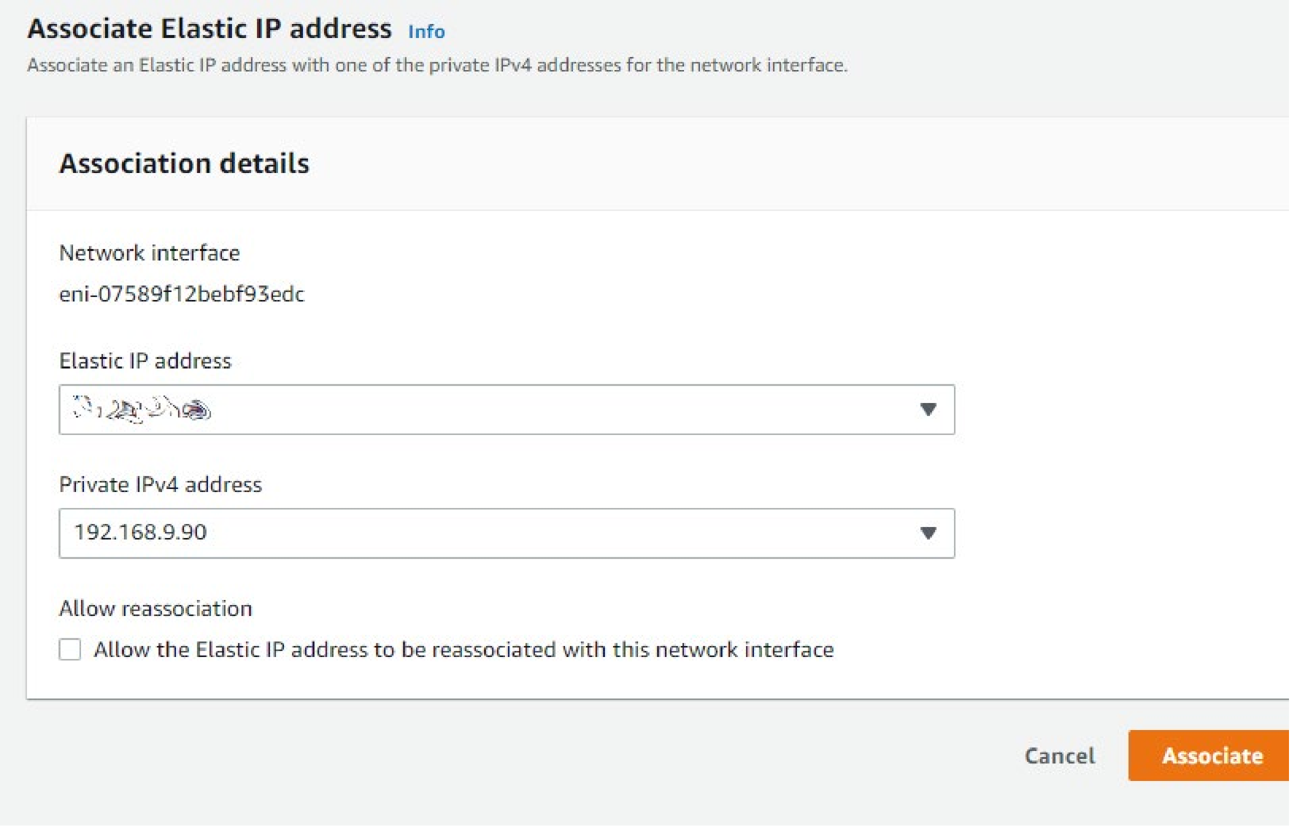
☑	Group ID	Group name	Description
☑	sg-03d8154ababea3025	SinemaRC_Securitygroups	Firewallrules

7. Click on "Create Network Interface".

Assigning the Elastic IP address to the network interface

1. Right-click on the name of the network interface.
2. Select "Associate Address".
3. For "Elastic IP address" select the desired IP address.

4. For "Private IPv4 address" select the IP address of the SINEMA RC server.



Associate Elastic IP address Info

Associate an Elastic IP address with one of the private IPv4 addresses for the network interface.

Association details

Network interface

eni-07589f12bebf93edc

Elastic IP address

[redacted] ▼

Private IPv4 address

192.168.9.90 ▼

Allow reassociation

□ Allow the Elastic IP address to be reassociated with this network interface

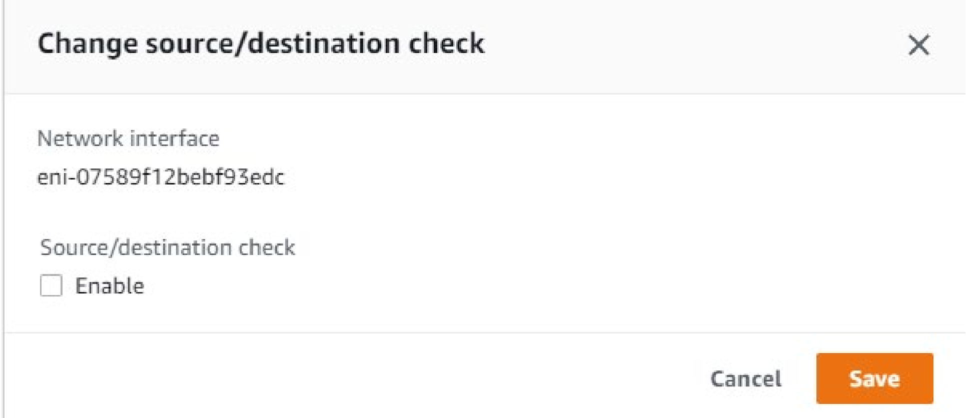
5. Click on "Associate".

Disable source/destination check

SINEMA RC does not support the check mechanism of AWS. To operate the instance without complications, disable the checks.

1. For "Network & Security", click on "Network Interfaces".
2. Right-click on the name of the network interface.
3. Select "Change source/des. check".

4. Select the "Enable" entry in the following dialog.



Change source/destination check

Network interface
eni-07589f12bebf93edc

Source/destination check
□ Enable

5. Click on "Save".

Additional information

AWS documentation "Amazon EC2" in the section "Work with network interfaces (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#working-with-enis)".

3.3.4 Starting the SINEMA RC instance

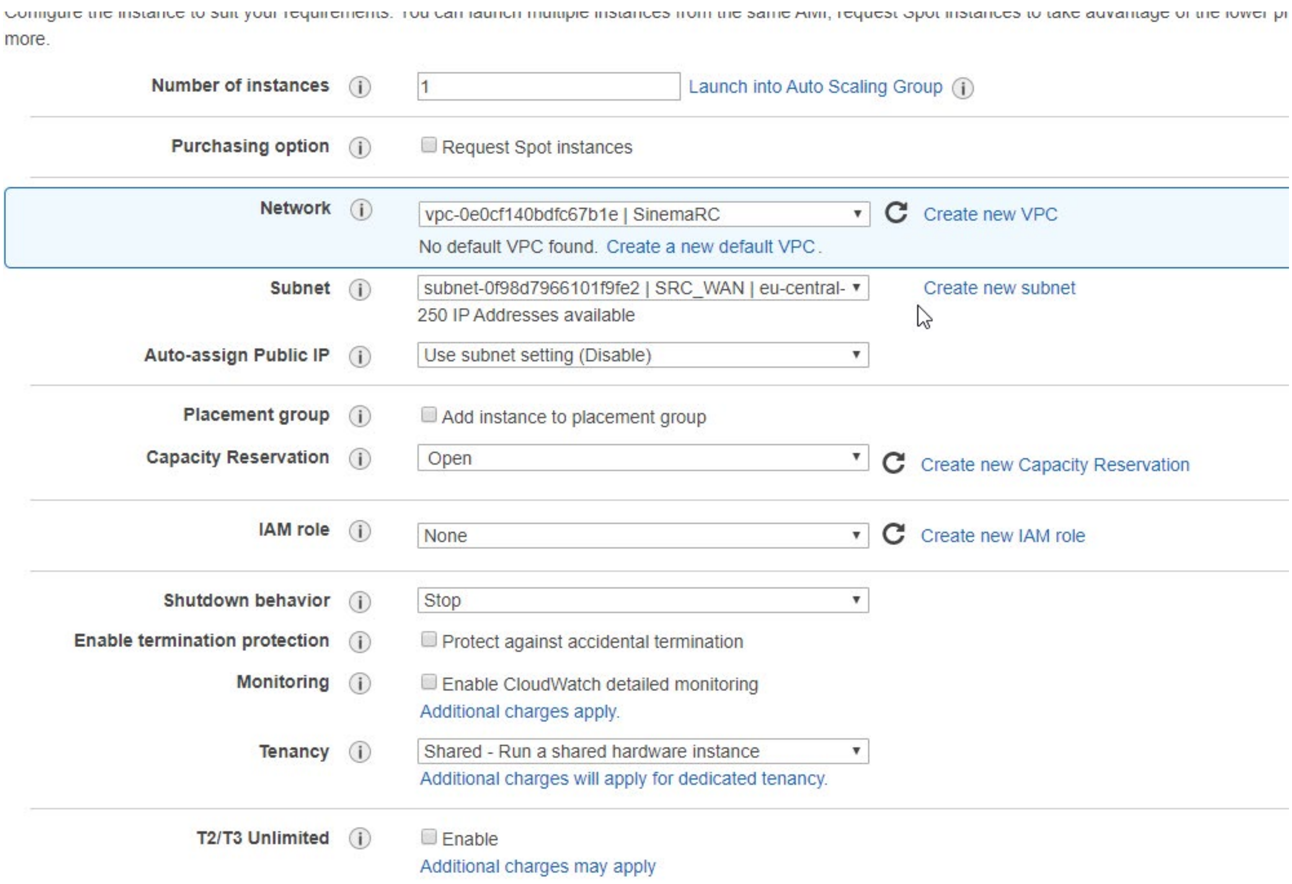
Requirement

- You have a valid AWS account, and you are logged in to the AWS management console.
- The EC2 dashboard is open.

Procedure

1. Under "Images", click on "AMI".
2. Select the SINEMA RC Server AMI and click on "Launch".
3. Select the type of instance and click on "Next: Configure Instance Details".
4. As "Network" select the configured VPC and as "Subnet" the configured SINEMA RC WAN subnet.

5. Under network interface, select the WAN network interface for eth0.



Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pr
more.

Number of instances ⓘ	1 — Launch into Auto Scaling Group ⓘ
Purchasing option ⓘ	□ Request Spot instances
Network ⓘ	vpc-0e0cf140bdfc67b1e | SinemaRC ▾ — Create new VPC No default VPC found. Create a new default VPC.
Subnet ⓘ	subnet-0f98d7966101f9fe2 | SRC_WAN | eu-central- ▾ — Create new subnet 250 IP Addresses available
Auto-assign Public IP ⓘ	Use subnet setting (Disable) ▾
Placement group ⓘ	□ Add instance to placement group
Capacity Reservation ⓘ	Open ▾ — Create new Capacity Reservation
IAM role ⓘ	None ▾ — Create new IAM role
Shutdown behavior ⓘ	Stop ▾
Enable termination protection ⓘ	□ Protect against accidental termination
Monitoring ⓘ	□ Enable CloudWatch detailed monitoring Additional charges apply.
Tenancy ⓘ	Shared - Run a shared hardware instance ▾ Additional charges will apply for dedicated tenancy.
T2/T3 Unlimited ⓘ	□ Enable Additional charges may apply

6. Click on "Review and Launch".

7. The connection authentication is queried on the next page.

8. Because the SINEMA RC can be used entirely with the WBM, an additional logon is not required and not even possible.

9. This means you select "Proceed without a key pair" and click on "Launch instances".

Additional information

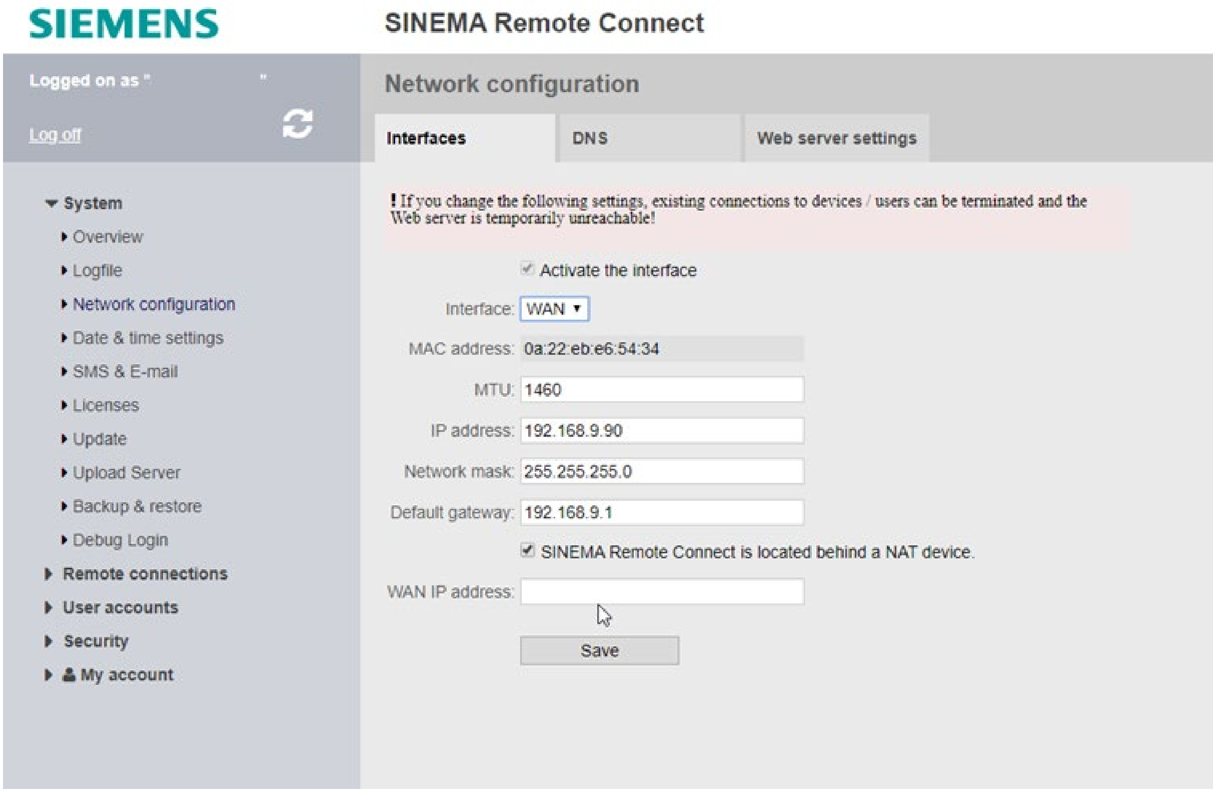
AWS documentation "Amazon EC2" in the section "Instances (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Instances.html)".

3.3.5 Configuring the SINEMA RC Server with cloud data

For the virtual machine to be reachable in the cloud, the ova file is uploaded and then converted into an Amazon Machine Image (AMI).

Procedure

1. Log in to SINEMA RC and go to "System > Network configurations".
2. Select "SINEMA Remote Connect is located behind a NAT device" and enter the "Elastic IP address" for "WAN IP address".



! If you change the following settings, existing connections to devices / users can be terminated and the Web server is temporarily unreachable!

☑ Activate the interface

Interface: WAN ▾

MAC address: 0a:22:eb:e6:54:34

MTU: 1460

IP address: 192.168.9.90

Network mask: 255.255.255.0

Default gateway: 192.168.9.1

☑ SINEMA Remote Connect is located behind a NAT device.

WAN IP address: