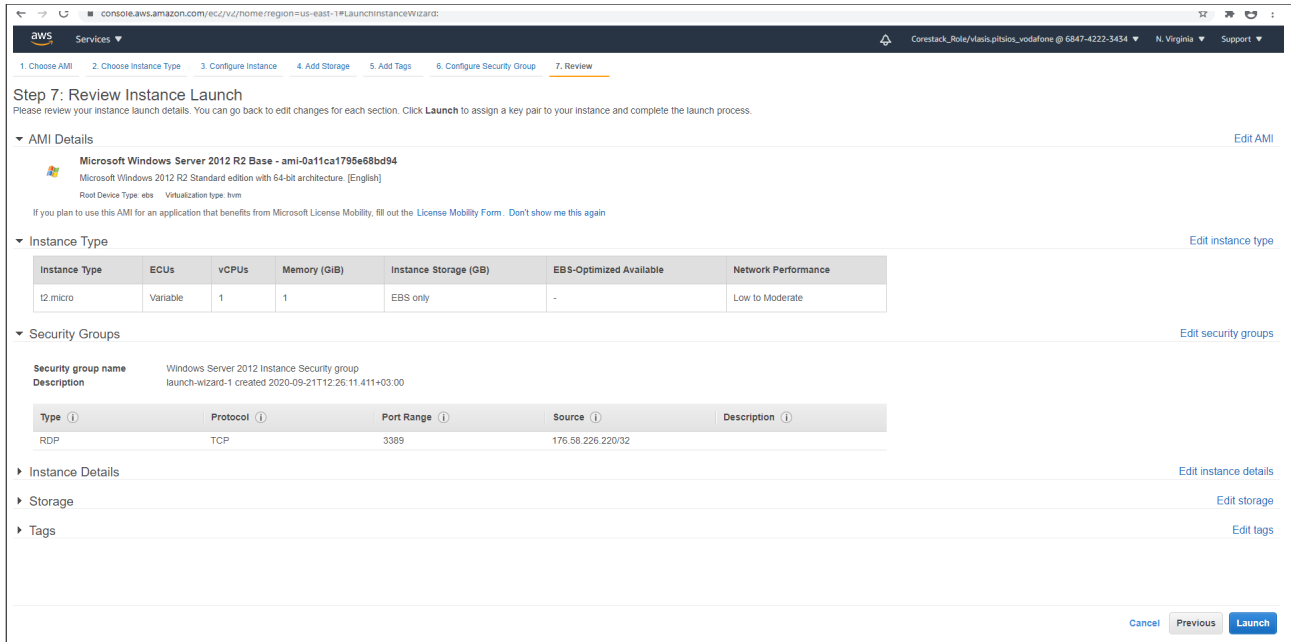


AWS Tech Essentials Project

Name: Vlasits Pitsios

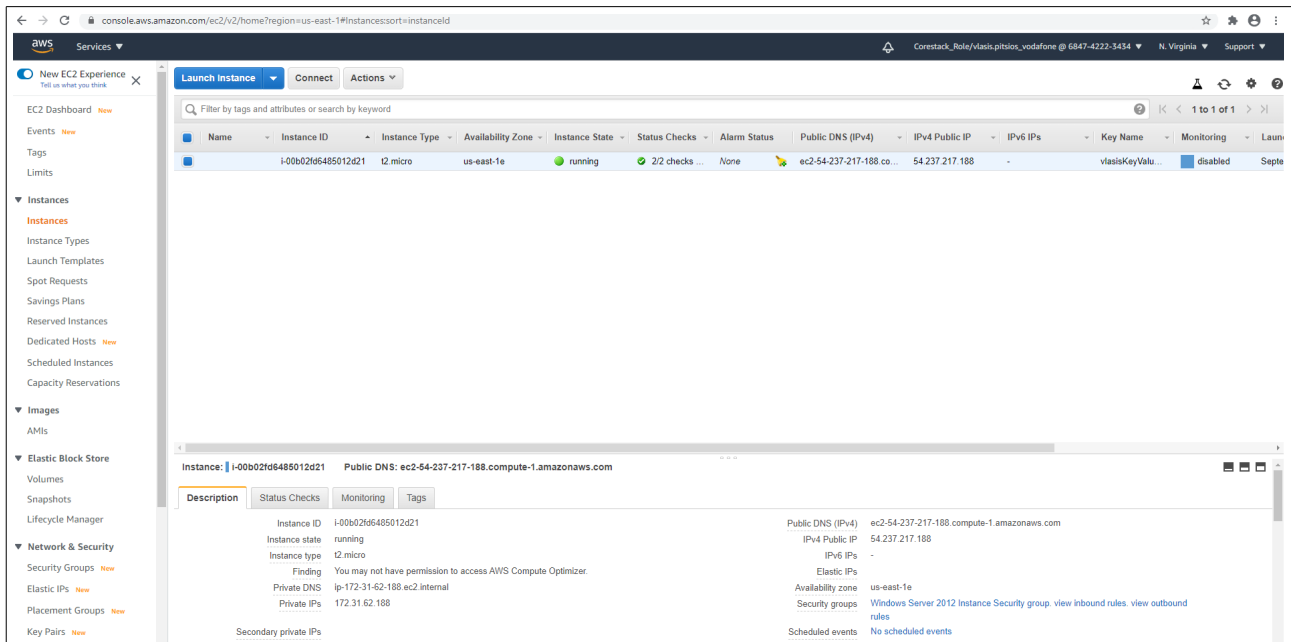
Email: vlasits.pitsios@vodafone.com

Company: Vodafone



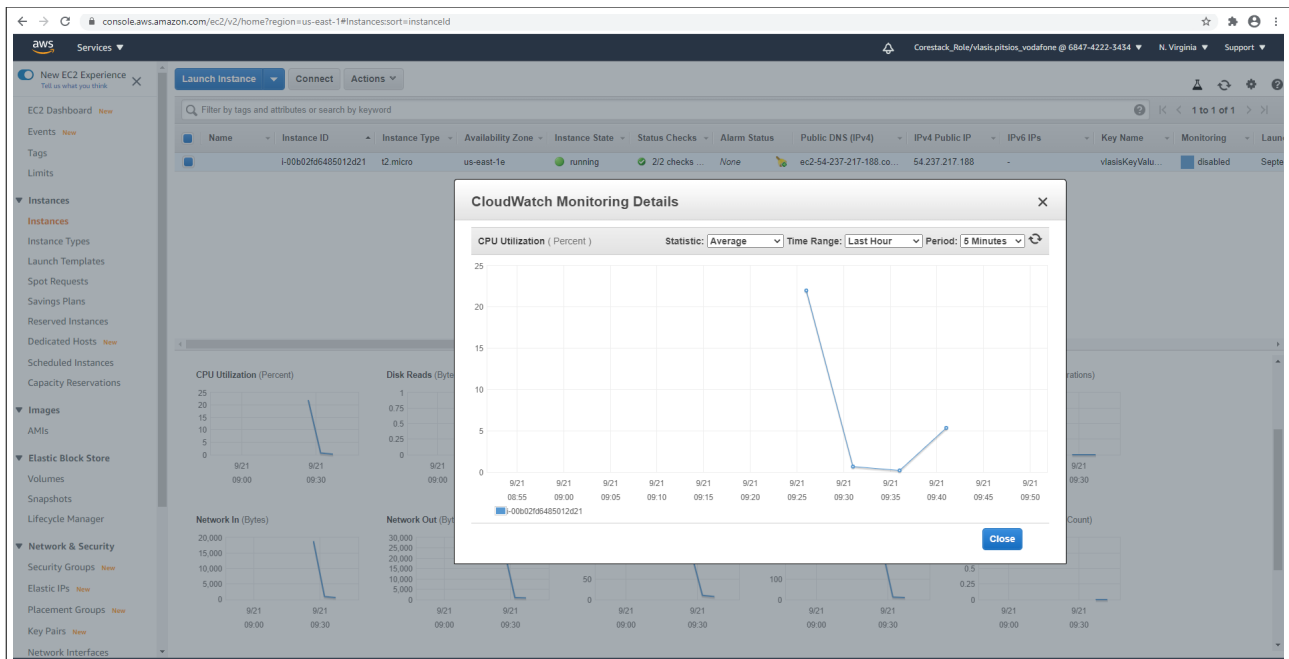
Screenshot 1 (Instance creation before launching)

Create an EC2 instance with Microsoft Windows Server 2012 R2 Base AMI.



Screenshot 2 (Instance Created)

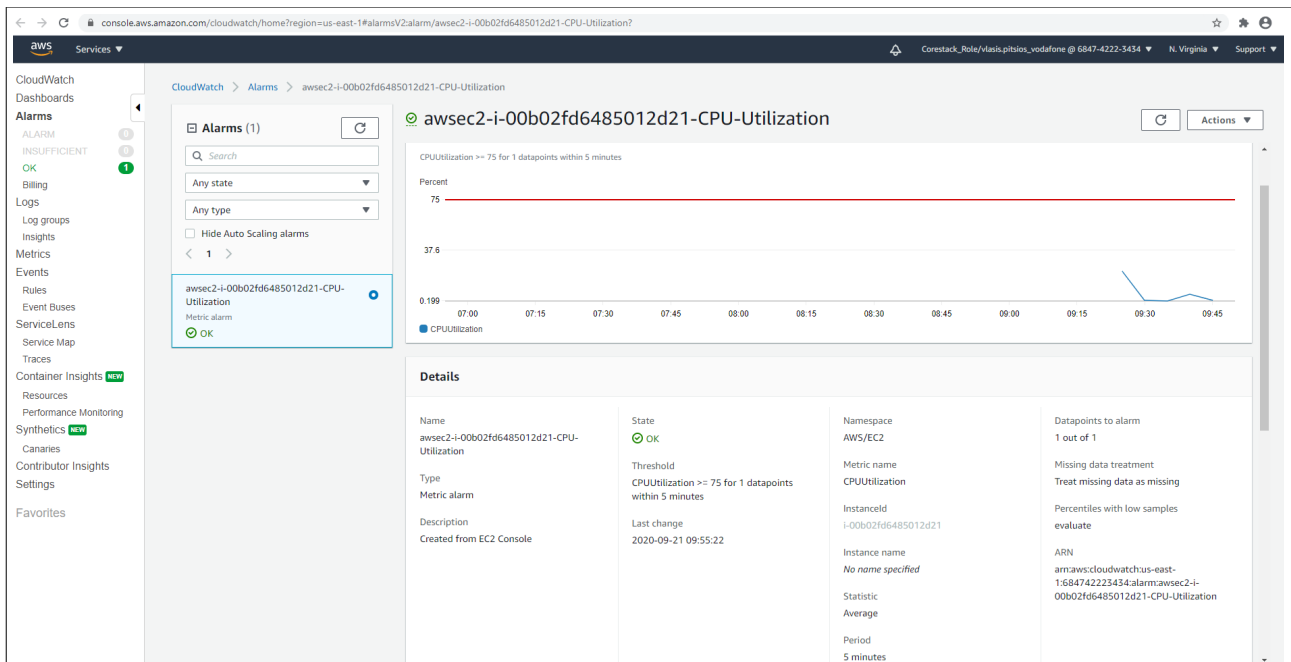
EC2 Instance is up and running



Screenshot 3 (CPU Utilization)
CPU Utilization screen

The screenshot shows the "Create Alarm" dialog in the AWS Management Console. The dialog is configured to create a CloudWatch alarm for "CPU Utilization Percent" on the instance "i-00b02f6d485012d21". The configuration includes: "Send a notification to" checked with the topic "cpuAlarmTopic"; "With these recipients" set to "user12345@vodafone.com"; "Take the action" unchecked; "Whenever" set to "Average" of "CPU Utilization"; the threshold "Is" set to ">= 75" Percent; "For at least" set to "1" consecutive period(s) of "5 Minutes"; and the "Name of alarm" set to "awssec2-i-00b02f6d485012d21-CPU-Utilization". A small preview graph on the right shows the metric's history. The background shows the instance details page with the "Monitoring" tab selected, indicating "No alarms configured".

Screenshot 4 (Alarma creation)
Create a CPU utilization alarm to send notifications on "cpuAlarmTopic" topic when the average CPU utilization is above 75% for at least 5 minutes.



Screenshot 5 (Alarm created)
Alarm is in status OK.

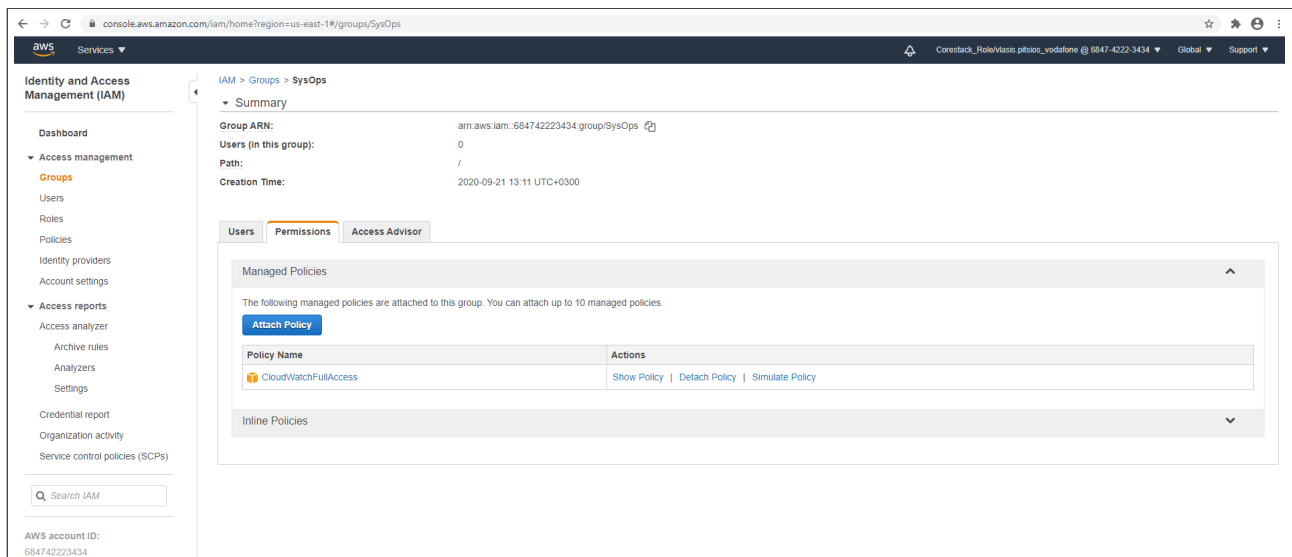
The screenshot shows the 'Add user' wizard in the AWS IAM console, specifically the 'Review' step (step 4 of 5). It displays the details of a user named 'monitorUser'. The user has 'Programmatic access and AWS Management Console access' and a 'Custom' console password type. The permissions summary shows that the user will be added to the 'IAMUserChangePassword' group. At the bottom, there are buttons for 'Cancel', 'Previous', and 'Create user'.

| User details | |
|------------------------|---|
| User name | monitorUser |
| AWS access type | Programmatic access and AWS Management Console access |
| Console password type | Custom |
| Require password reset | Yes |
| Permissions boundary | Permissions boundary is not set |

| Permissions summary | |
|---|-----------------------|
| The user shown above will be added to the following groups. | |
| Type | Name |
| Managed policy | IAMUserChangePassword |

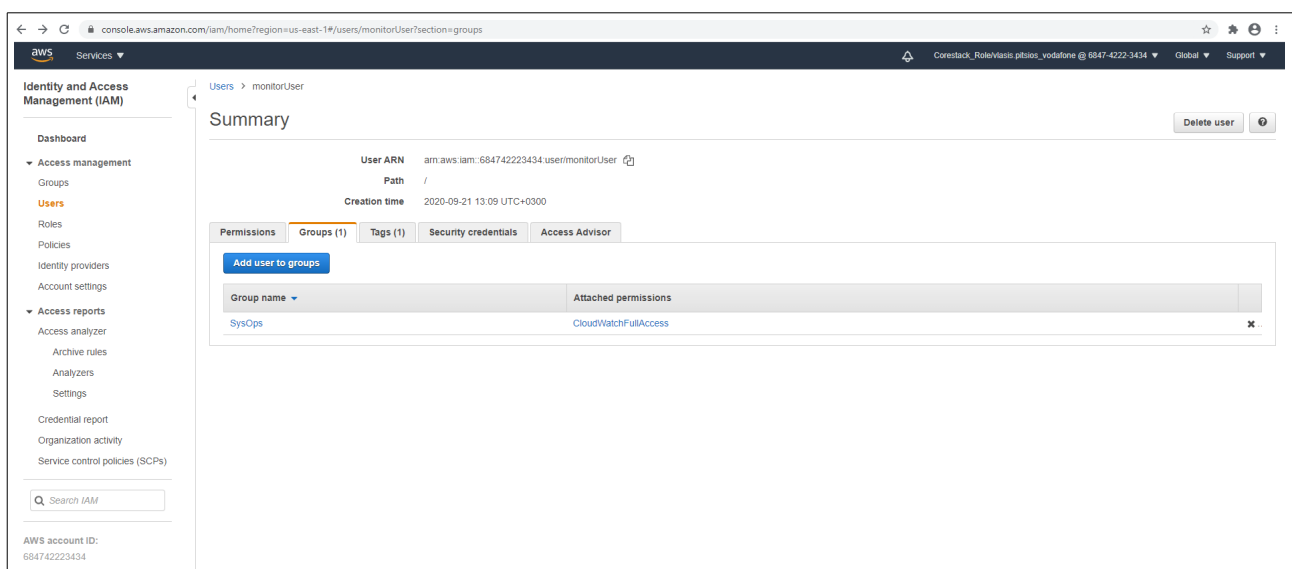
| Tags | |
|---|---------------|
| The new user will receive the following tag | |
| Key | Value |
| system | administrator |

Screenshot 6 (User creation)
Create user with name "monitorUser"



Screenshot 7 (Group created)

Group with name "SysOps" was created with full access to Cloudwatch.



Screenshot 8 (attach user on a group)

User "monitorUser" is attached to "SysOps" group in order to have full access to CloudWatch

console.aws.amazon.com/iam/home#/roles/new?step=review&commonUseCase=EC2%2BEC2&selectedUseCase=EC2&policies=arn:aws:iam::aws:policy%2FAmazonS3FullAccess

aws Services

Corestack_Role/viasis.pitstos_vodafone

Create role

1 2 3 4

Review

Provide the required information below and review this role before you create it.

Role name*

Use alphanumeric and '+', '-', '@', '_' characters. Maximum 64 characters.

Role description

Maximum 1000 characters. Use alphanumeric and '+', '-', '@', '_' characters.

Trusted entities AWS service: ec2.amazonaws.com

Policies AmazonS3FullAccess [View](#)

Permissions boundary Permissions boundary is not set

The new role will receive the following tag

| Key | Value |
|------|---------------|
| name | ec2AccessToS3 |

* Required

Cancel Previous **Create role**

Screenshot 9 (role creation)

Create S3 Full access role from EC2 instance named as "ec2AccessToS3".

console.aws.amazon.com/ec2/v2/home?region=us-east-1#Instances:sort=instanceId

aws Services

Corestack_Role/viasis.pitstos_vodafone @ 6847-4222-3434 N, Virginia Support

New EC2 Experience Tell us what you think

Launch Instance Connect Actions

Filter by tags and attributes or search by keyword

| Name | Instance ID | Instance Type | Availability Zone | Instance State | Status Checks | Alarm Status | Public DNS (IPv4) | IPv4 Public IP | IPv6 IPs | Key Name | Monitoring |
|------|---------------------|---------------|-------------------|----------------|----------------|--------------|--------------------------|----------------|----------|------------------|------------|
| | i-00b02fd6485012d21 | t2.micro | us-east-1e | running | 2/2 checks ... | OK | ec2-54-237-217-188.co... | 54.237.217.188 | - | viasisKeyValu... | disabled |

Instances

Instance state: running

Instance type: t2.micro

Finding: You may not have permission to access AWS Compute Optimizer.

Private DNS: ip-172-31-62-188.ec2.internal

Private IPs: 172.31.62.188

Secondary private IPs

VPC ID: vpc-526d952f

Platform: Windows

Platform details: Windows

Usage operation: RunInstances.0002

Source/dest. check: True

T2/T3 Unlimited: Disabled

EBS-optimized: False

Root device type: ebs (i)

Root device: /dev/sda1

Block device mapping: /dev/nvda1

IPv4 Public IP: 54.237.217.188

IPv6 IPs: -

Elastic IPs: -

Availability zone: us-east-1e

Security groups: Windows_Server_2012-R2_RTM-English_A4Bt-Base-2020.09.09 (ami-0a11ca1795e68bd94) subnet-302d9e01

Scheduled events: No scheduled events

AMI ID: Windows_Server-2012-R2_RTM-English_A4Bt-Base-2020.09.09 (ami-0a11ca1795e68bd94)

Subnet ID: subnet-302d9e01

Network interfaces: eni0

IAM role: **ec2AccessToS3**

Key pair name: viasisKeyValu...

Owner: 684742223434

Launch time: September 21, 2020 at 12:31:16 PM UTC+3 (1 hour)

Termination protection: False

Lifecycle: normal

Monitoring: basic

Screenshot 10 (Attach role to EC2 instance)

Attach "ec2AccessToS3" role to EC2 instance with instance ID i-00b02fd6485012d21