



EC2 Instance Start & Stop Using CloudWatch Rule as a target using SSMAutomations

—

Prepared by: Singaravelan.P
Reviewed by:
Accepted By:

Table of contents

Table of contents	1
Overview	1
EC2 Stop & Start	2
Goals	2
Step 1: Create an IAM Role for EC2 Instance SSM Full Access	2
Step 2: Attach a IAM Role for EC2 Instance	4
Step 3: Install the SSM Agent in your EC2 Instances	4
Step 4: Create a IAM role for AutomationAssumeRole for Cloudwatch target SSMAutomation	5
Step 5: Create a Cloudwatch rule for EC2 instance Start	7

Overview

EC2 Start & Stop:

This scenario is Start & Stop an EC2 instance in Specific time for each server using SSM Automation with Cloudwatch rule.

Goals

1. Create a IAM role(SSM_Full) for EC2 instance role policy is SSM Full Access
2. Attach a SSM_Full role to Specified EC2 Instance
3. Install a SSM Agent in All EC2 instance
4. Create a IAM role for AutomationAssumeRole for Cloudwatch target SSMAutomation
5. Create a Cloudwatch rule for EC2 instance stop
6. Create a Cloudwatch rule for EC2 instance start

Step1: Create an IAM Role for EC2 Instance SSM Full Access:

Go to IAM Console create a Role for EC2 with SSM Full Access.

Create role

Select type of trusted entity

AWS service
EC2, Lambda and others

Another AWS account
Belonging to you or 3rd party

Web Identity
Cognito or any OpenID provider

SAML 2.0 federation
Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose the service that will use this role

EC2
Allows EC2 instances to call AWS services on your behalf.

Lambda
Allows Lambda functions to call AWS services on your behalf.

API Gateway CodeDeploy EMR KMS RoboMaker
AWS Backup CodeGuru Elasticache Kinesis S3

* Required Cancel Next: Permissions

Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy

Filter policies Showing 1 result

Policy name	Used as
<input checked="" type="checkbox"/> AmazonSSMFullAccess	Permissions policy (10)

Provide a Role name & review to create

Create role

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.

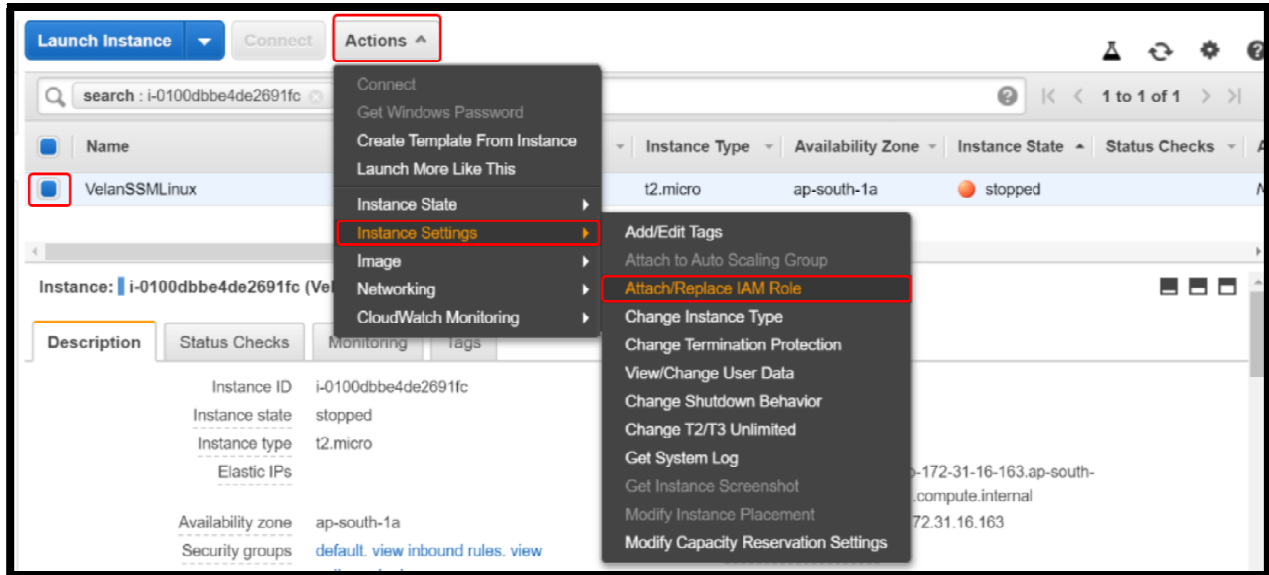
Trusted entities AWS service: ec2.amazonaws.com

Policies AmazonSSMFullAccess

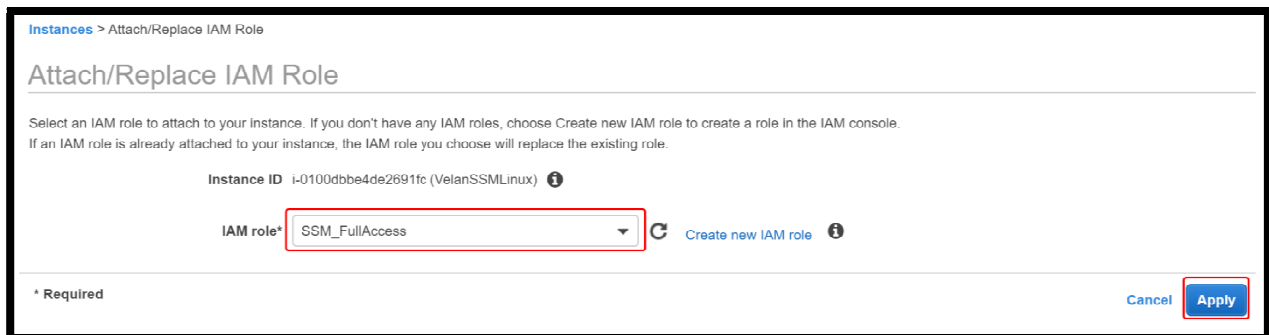
* Required Cancel Previous **Create role**

Step2: Attach a IAM Role for EC2 Instance

Go to Ec2 -> Choose a Instance -> Action-> Instance Setting-> Attach/Replace IAM role



Then choose your SSM Role name & Apply.



Step3: Install the SSM Agent in your EC2 Instances

Refer the below link to install the agent.

<https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-manual-agent-install.html>

After installation check the ssm gent service is running & enable

Note : Latest AMI it will come by default in SSM.

Step4: Create a IAM role for AutomationAssumeRole for Cloudwatch target SSMAutomation

Go to IAM Console create a Role (SSMAutomationRole) for EC2 with AmazonSSMAutomationRole

Create role 1 2 3 4

Select type of trusted entity

AWS service
EC2, Lambda and others

Another AWS account
Belonging to you or 3rd party

Web identity
Cognito or any OpenID provider

SAML 2.0 federation
Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose the service that will use this role

EC2
Allows EC2 instances to call AWS services on your behalf.

Lambda
Allows Lambda functions to call AWS services on your behalf.

API Gateway CodeDeploy EMR KMS RoboMaker
AWS Backup CodeGuru ElastiCache Kinesis S3

* Required Cancel **Next: Permissions**

Attach permissions policies (AmazonSSMAutomationRole)

Create role 1 2 3 4

▼ Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy ↻

Filter policies AmazonSSMAutomationRole Showing 1 result

	Policy name	Used as
<input checked="" type="checkbox"/>	AmazonSSMAutomationRole	Permissions policy (1)

* Required Cancel Previous **Next: Tags**

Provide a role name & review to create

Create role

1234

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  [AmazonSSMAutomationRole](#) 

* Required

[Cancel](#) [Previous](#) [Create role](#)

Go to the role (SSMAutomationRole) & click the Trust relationships to edit following

Edit trust relationship

Trusted entities

The following trusted entities can assume this role.

Trusted entities

The identity provider(s) ec2.amazonaws.com

The identity provider(s) ssm.amazonaws.com

```
"Service": [  
  "ec2.amazonaws.com",  
  "ssm.amazonaws.com"  
]
```

Step5: Create a Cloudwatch rule for EC2 instance Stop

Go to Cloudwatch -> Events -> rules -> Create rule

Click a Schedule with Cron expression and provide a time to Stop

Step 1: Create rule

Create rules to invoke Targets based on Events happening in your AWS environment.

Event Source

Build or customize an Event Pattern or set a Schedule to invoke Targets.

☐ Event Pattern ☒ **Schedule**

☐ Fixed rate of

☒ **Cron expression**

Next 10 Trigger Date(s)

1. Thu, 30 Jan 2020 05:30:00 GMT

In the Same Page Click the target -> add target -> SSM Automation

Collect an SSMAutomationRole ARN

Roles > SSMAutomationRole

Summary

Role ARN	arn:aws:iam::872599169723:role/SSMAutomationRole
Role description	Allows EC2 instances to call AWS services on your behalf. Edit
Instance Profile ARNs	arn:aws:iam::872599169723:instance-profile/SSMAutomationRole

Then choose your document for AWS-StopEC2Instance and Instance Role ARN.

Targets

Select Target to invoke when an event matches your Event Pattern or when schedule is triggered.

SSM Automation

Document* **AWS-StopEC2Instance**

► Configure document version

▼ Configure automation parameter(s)

☐ No Parameter(s) ⓘ

☒ Constant ⓘ

InstanceId* **i-0100dbbe4de2691fc**

AutomationAssumeRole **arn:aws:iam::872599169723:role/SSMAutomationRole**

☐ Input Transformer ⓘ

CloudWatch Events needs permission to call SSM Start Automation Execution with your supplied Automation document and parameters. By continuing, you are allowing us to do so.

☒ Create a new role for this specific resource

AWS_Events_Invoke_Start_Automation_Execution_1292825222

☐ Use existing role ⓘ

[Learn more](#) about CloudWatch Events identity-based policies.

Add target*

Cancel **Configure details**

Click to Configure & provide a Role name with Description, Then Click to Create rule

Rule definition

Name* **EC2-Stop-DemoLinux**

Description **The instance will Stop every day 5:30 GMT**

State ☒ Enabled

* Required

Cancel **Back** **Create rule**

Rule is Created Successfully.

☐ ☒ **EC2-Stop-DemoLinux** **The instance will Stop every day 5:30 GMT**

Step5: Create a Cloudwatch rule for EC2 instance Start

Go to Cloudwatch -> Events -> rules -> Create rule



Click a Schedule with Cron expression and provide a time to Start

Step 1: Create rule

Create rules to invoke Targets based on Events happening in your AWS environment.

Event Source

Build or customize an Event Pattern or set a Schedule to invoke Targets.

☐ Event Pattern  ☒ Schedule 

☐ Fixed rate of

☒ Cron expression

Next 10 Trigger Date(s)



1. Wed, 29 Jan 2020 15:30:00 GMT

In the Same Page Click the target -> add target -> SSM Automation

Collect an SSMAutomationRole ARN

Roles > SSMAutomationRole

Summary

Role ARN	arn:aws:iam::872599169723:role/SSMAutomationRole 
Role description	Allows EC2 instances to call AWS services on your behalf. Edit
Instance Profile ARNs	arn:aws:iam::872599169723:instance-profile/SSMAutomationRole 

Then choose your document for AWS-StartEC2Instance and Instanced Role ARN.

Targets

Select Target to invoke when an event matches your Event Pattern or when schedule is triggered.

SSM Automation

Document*

AWS-StartEC2Instance

Configure document version

Configure automation parameter(s)

☐ No Parameter(s)
☒ Constant

Instanced*

i-0100dbbe4de2691fc

AutomationAssumeRole

arn:aws:iam::872599169723:role/SSMAutomationRole

☐ Input Transformer

CloudWatch Events needs permission to call SSM Start Automation Execution with your supplied Automation document and parameters. By continuing, you are allowing us to do so.

☒ Create a new role for this specific resource

AWS_Events_Invoke_Start_Automation_Execution_1023174702

☐ Use existing role

[Learn more](#) about CloudWatch Events identity-based policies.

Add target*

Cancel
Configure details

Click to Configure & provide a Role name with Description, Then Click to Create rule

Rule definition

Name*

EC2-Start-DemoLinux

Description

This instance will start every day 15:30 GMT

State
☒ Enabled

* Required

Cancel
Back
Create rule

Rule is Created Successfully.

☐
☒

EC2-Stop-DemoLinux

The instance will Stop every day 5:30 GMT