

# Configure the EC2 plugin

Video 6.4

# What you will learn in this video

**Theory:**

# What you will learn in this video

## Theory:

- EC2 plugin

# What you will learn in this video

## Theory:

- EC2 plugin
- IAM user and policy

# What you will learn in this video

## Theory:

- EC2 plugin
- IAM user and policy
- AMI

# What you will learn in this video

## Theory:

- EC2 plugin
- IAM user and policy
- AMI

## Practice:

# What you will learn in this video

## Theory:

- EC2 plugin
- IAM user and policy
- AMI

## Practice:

- Create a IAM policy and user with credentials AWS

# What you will learn in this video

## Theory:

- EC2 plugin
- IAM user and policy
- AMI

## Practice:

- Create a IAM policy and user with credentials AWS
- Add AWS credentials to Jenkins



# What you will learn in this video

## Theory:

- EC2 plugin
- IAM user and policy
- AMI

## Practice:

- Create a IAM policy and user with credentials AWS
- Add AWS credentials to Jenkins
- Whitelist an IP address in the security group

# What you will learn in this video

## Theory:

- EC2 plugin
- IAM user and policy
- AMI

## Practice:

- Create a IAM policy and user with credentials AWS
- Add AWS credentials to Jenkins
- Whitelist an IP address in the security group
- Install and configure the EC2 plugin

# Amazon EC2 Plugin

## Amazon EC2 Plugin

- It allows Jenkins to **automatically start slave nodes** on EC2 instances **on demand**

## Amazon EC2 Plugin

- It allows Jenkins to **automatically start slave nodes** on EC2 instances **on demand**
- It allows to **automatically decommission EC2 instances** as they get unused

## Amazon EC2 Plugin

- It allows Jenkins to **automatically start slave nodes** on EC2 instances **on demand**
- It allows to **automatically decommission EC2 instances** as they get unused
- It allows to **configure the type of slave nodes**, the AWS **region** where to start them, the **idle time** after which they can be decommissioned, etc.



# IAM

- IAM stands for **Identify and Access Management**



# IAM

- IAM stands for **Identify and Access Management**
- IAM enables to **access AWS services and resources securely**

# IAM

- IAM stands for **Identify and Access Management**
- IAM enables to **access AWS services and resources securely**
- IAM is used to **create users and permissions**

# IAM

- IAM stands for **Identify and Access Management**
- IAM enables to **access AWS services and resources securely**
- IAM is used to **create users and permissions**
- A **IAM policy is a set of permissions** attached to a user or a resource

# IAM

- IAM stands for **Identify and Access Management**
- IAM enables to **access AWS services and resources securely**
- IAM is used to **create users and permissions**
- A **IAM policy is a set of permissions** attached to a user or a resource
- IAM policies are **stored as JSON files**

# IAM

- IAM stands for **Identify and Access Management**
- IAM enables to **access AWS services and resources securely**
- IAM is used to **create users and permissions**
- A **IAM policy** is a **set of permissions** attached to a user or a resource
- IAM policies are **stored as JSON files**
- We are going to create a **IAM policy** and a **IAM user** to **grant access to AWS from Jenkins**



- AMI stands for **Amazon Machine Image**

- AMI stands for **Amazon Machine Image**
- A master image or **template to create virtual servers** in AWS



- AMI stands for **Amazon Machine Image**
- A master image or **template to create virtual servers** in AWS
- We are going to create an **AMI to provide a base image for the slave node**

## Prerequisites

## Prerequisites

- Open the IAM Policy at [https://github.com/cirulls/hands-on-jenkins/blob/master/section\\_6/code/policy-jenkins-slave-node.json](https://github.com/cirulls/hands-on-jenkins/blob/master/section_6/code/policy-jenkins-slave-node.json)

## Prerequisites

- Open the IAM Policy at [https://github.com/cirulls/hands-on-jenkins/blob/master/section\\_6/code/policy-jenkins-slave-node.json](https://github.com/cirulls/hands-on-jenkins/blob/master/section_6/code/policy-jenkins-slave-node.json)
- Open the SSH private key created in video 6.2

## Prerequisites

- Open the IAM Policy at [https://github.com/cirulls/hands-on-jenkins/blob/master/section\\_6/code/policy-jenkins-slave-node.json](https://github.com/cirulls/hands-on-jenkins/blob/master/section_6/code/policy-jenkins-slave-node.json)
- Open the SSH private key created in video 6.2
- Open the csv file with AWS credentials (we will create it in this video)



- Create a IAM policy and IAM user with credentials in AWS

- Create a IAM policy and IAM user with credentials in AWS
- Add AWS credentials in Jenkins



- Create a IAM policy and IAM user with credentials in AWS
- Add AWS credentials in Jenkins
- Whitelist Jenkins' IP address inside the security group

- Create a IAM policy and IAM user with credentials in AWS
- Add AWS credentials in Jenkins
- Whitelist Jenkins' IP address inside the security group
- Install the EC2 plugin

- Create a IAM policy and IAM user with credentials in AWS
- Add AWS credentials in Jenkins
- Whitelist Jenkins' IP address inside the security group
- Install the EC2 plugin
- Configure the EC2 plugin

# Next Video

Video 6.5 Run Jobs on a Slave Node

