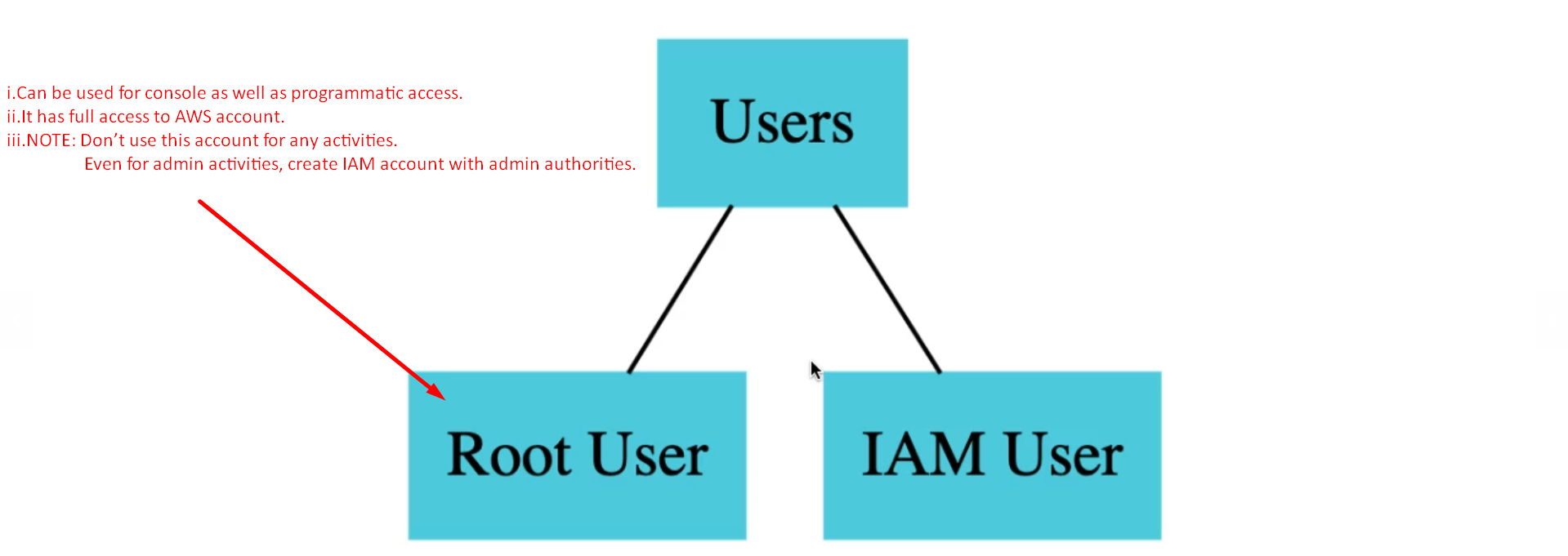
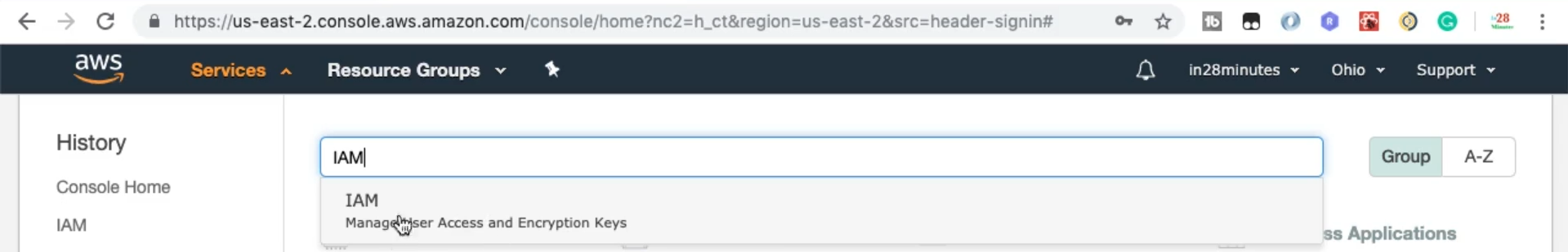
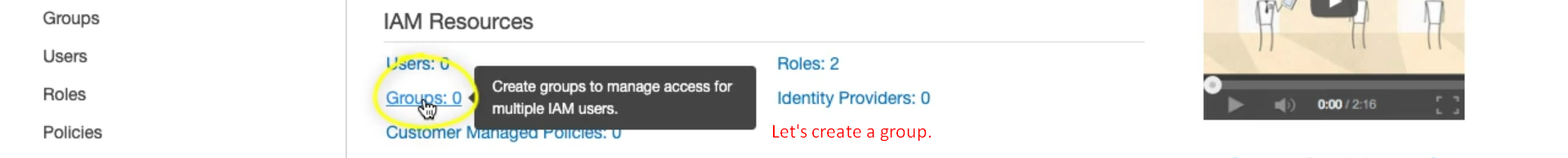
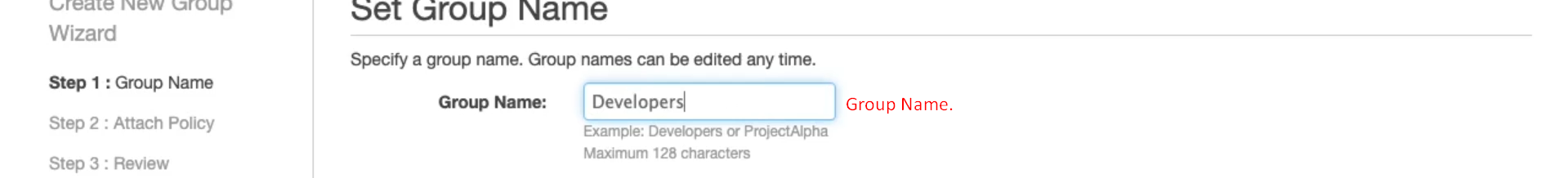
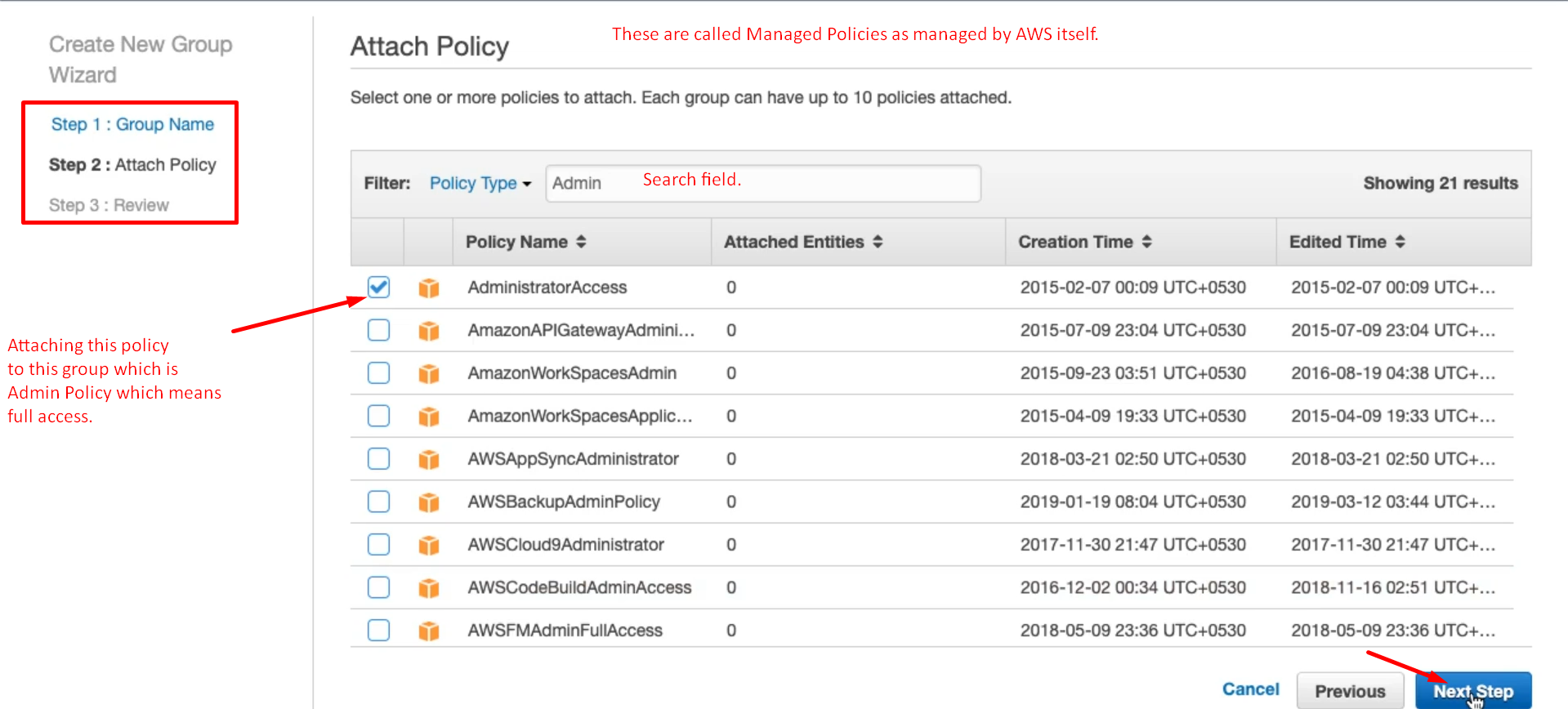
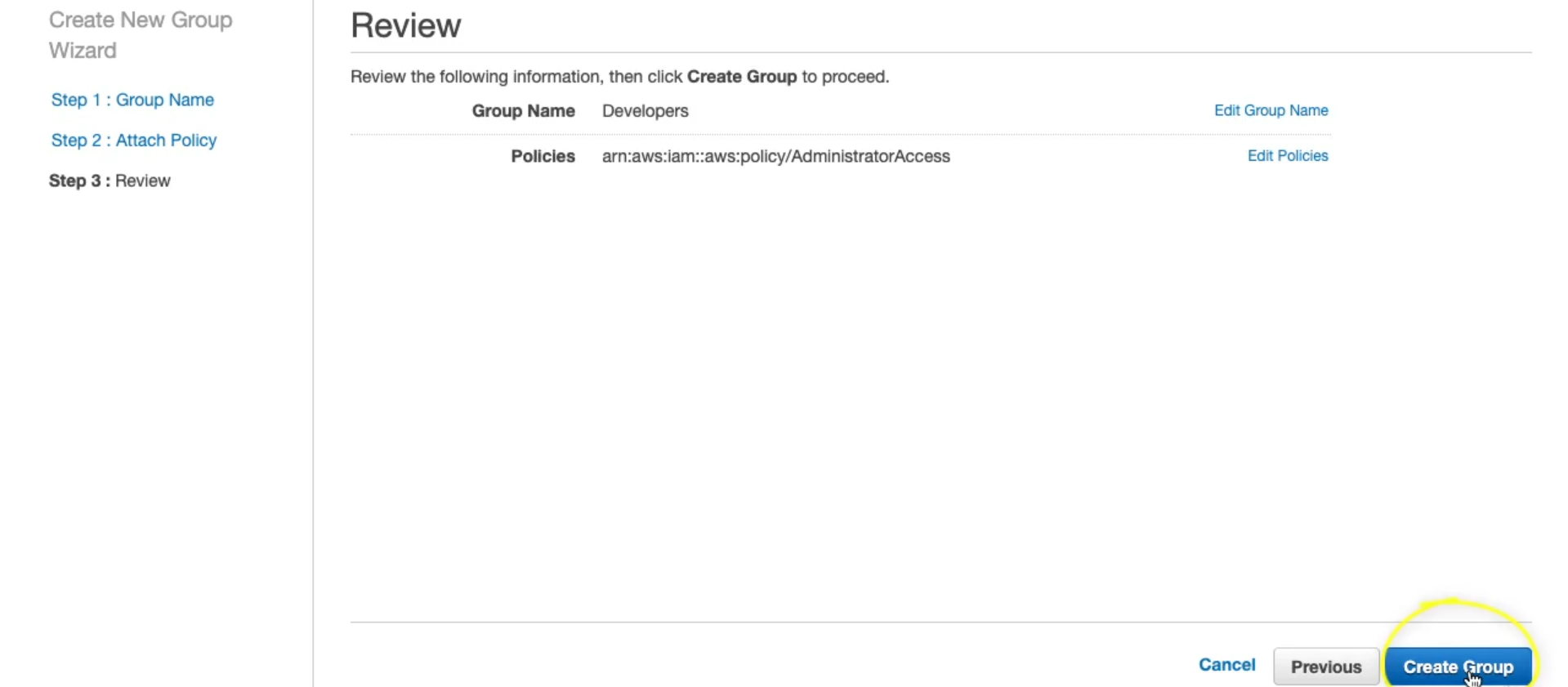
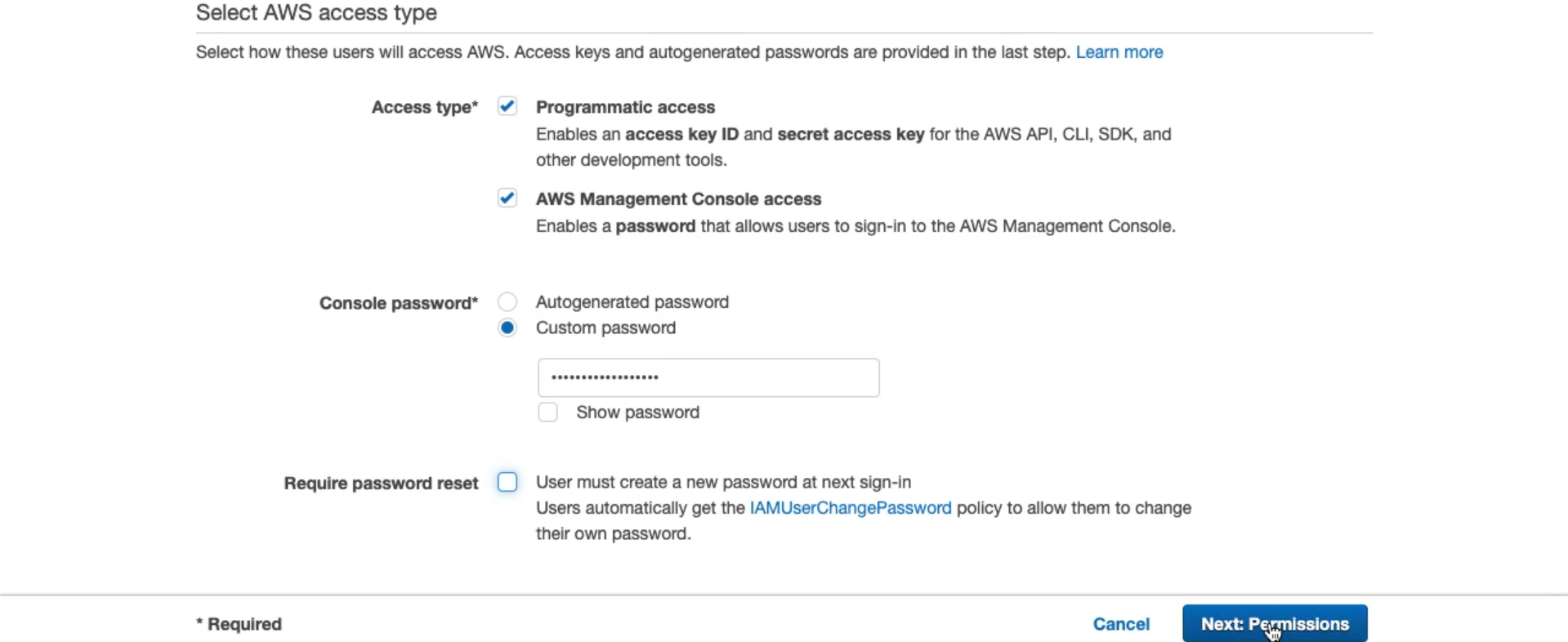
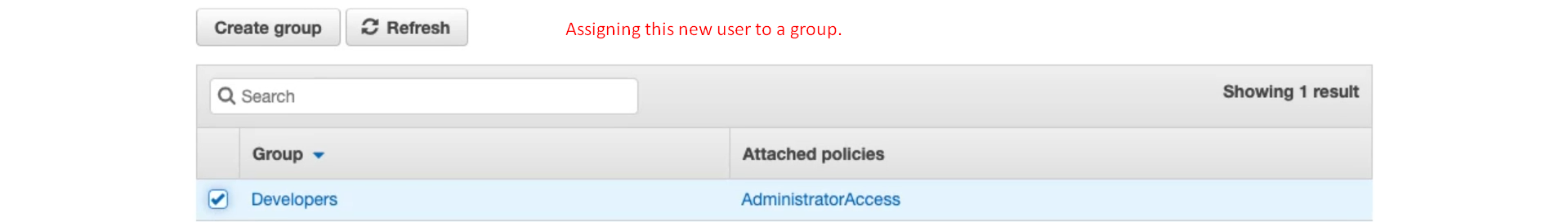
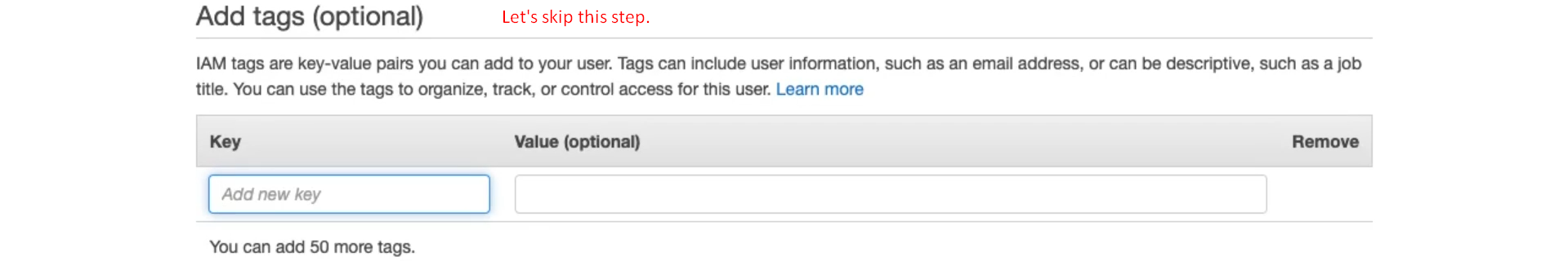
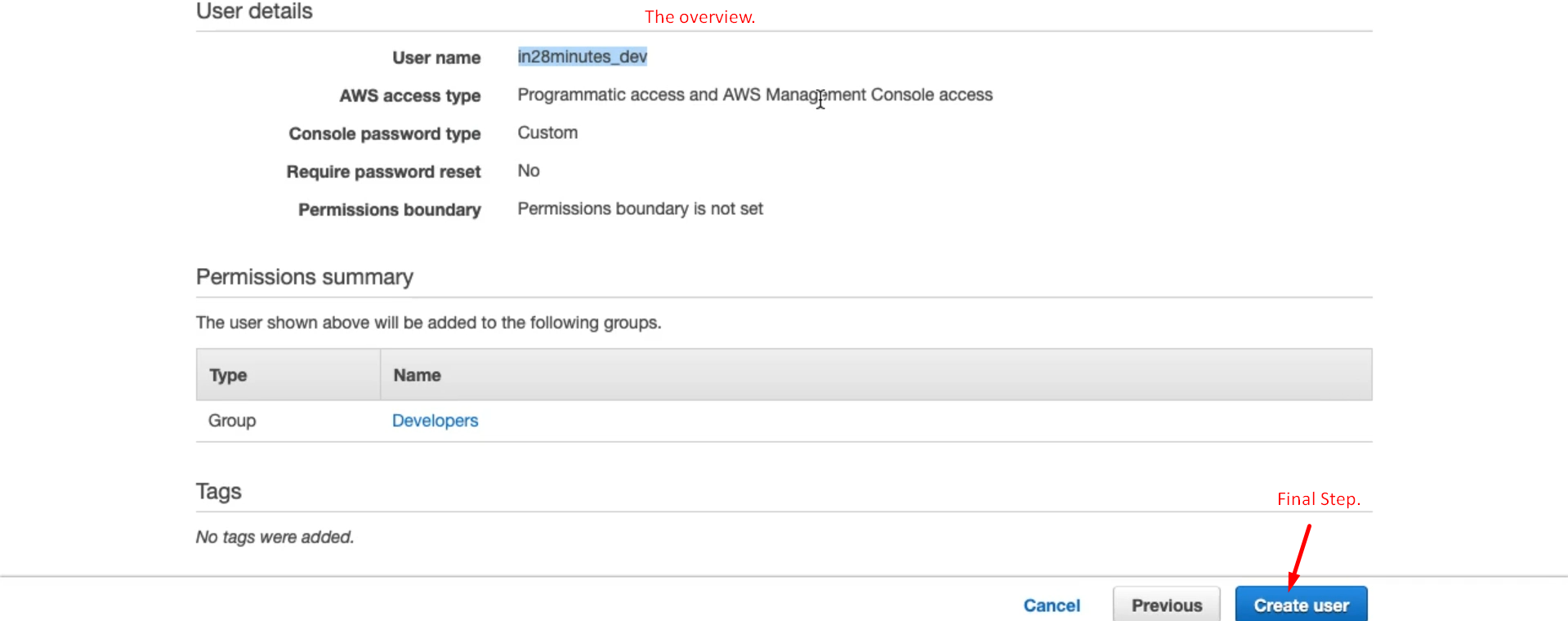
1. So far, we created AWS account which is Root Account.
2. Let’s secure it by creating IAM user.  
   
3. Let’s learn how to create IAM user and how to use IAM user for all AWS activities.
4. **Users**:  
   
   1. **Root User**:
      1. Can be used for console as well as programmatic access.
      2. It has full access to AWS account.
      3. NOTE: Don’t use this account for any activities.   
         Even for admin activities, create IAM account with admin authorities.
   2. **IAM User**:
5. Let’s see how to create IAM account.  
     
   
6. Policies (Authorities) can be assigned to either direct IAM user or a group.
7. 
8. 
9. Let’s assign some policies to this group.
   1. There are predefined policies called 🡺 Managed Policies as managed by AWS.
   2. 
   3. 
10. Let’s create and add a new user to this Group.
    1. 
    2. Actually, there are two kinds of users who may be accessing AWS service and performing an action.
       1. Programs: They create resources in AWS.
       2. A living user himself: They access through GUI (AWS Management Console)
    3. On user form, let’s fill the data for the new user.   
         
       
    4. Let’s assign this user to a group.  
       
    5. 
    6. 
    7. 