Blogs

Told you, we love sharing!

Category

ENTER EMAIL	Subscribe to Our Blog

CHEF recipe to change pem file of running ec2 instances and adding a new user to all the instances and give sudo privileges

AWS (HTTP://WWW.TOTHENEW.COM/BLOG/CATEGORY/TECHNOLOGY/AWS-2/), CHEF (HTTP://WWW.TOTHENEW.COM/BLOG/CATEGORY/TECHNOLOGY/DEVOPS-TECHNOLOGY/CHEF-DEVOPS/)

07 / APR / 2015   BY SHARAD AGGARWAL (HTTP://WWW.TOTHENEW.COM/BLOG/AUTHOR/SHARADAINTELLIGRAPE-COM/)   0 COMMENTS (HTTP://WWW.TOTHENEW.COM/BLOG/CHEF-RECIPE-TO-CHANGE-PEM-FILE-OF-RUNNING-EC2-INSTANCES-AND-ADDING-A-NEW-USER-TO-ALL-THE-INSTANCES-AND-GIVE-SUDO-PRIVILEGES/#RESPOND)

Share this blog

Email   Twitter   Facebook   LinkedIn   Google+

This blog is to enable AWS chef professionals (http://www.tothenew.com/devops-engineers-developers-team) to change pem of running servers or to add a new user with sudo privileges to an EC2 server farm using chef (http://www.tothenew.com/devops-chef-puppet-docker). The post actually refers to a production usecase in which there is a huge number of instances running on single or multiple pem files which needed to be replaced instantly to a single pem file for all the servers without any downtime. This can be done to overcome security issue, for example, the pem file is being rotated to different peoples or the person who was managing these servers and there keys left the organization.

Quick and easy resolution for above concern is listed below,

1) This blogpost assumes pre existing CHEF test environment of 3 ubuntu servers, a chef server, a chef client and a chef workstation. For more information on setting up above mentioned test environment, please refer link below,
https://www.digitalocean.com/community/tutorials/how-to-install-a-chef-server-workstation-and-client-on-ubuntu-vps-instances (https://www.digitalocean.com/community/tutorials/how-to-install-a-chef-server-workstation-and-client-on-ubuntu-vps-instances)

2) Create a new keypair using AWS console and download the new pem file,

3) Obtain a public key against recently downloaded pem key using below command,

```
intelligrape@sharad: ~
intelligrape@sharad:~$ ssh-keygen -y
Enter file in which the key is (/home/intelligrape/.ssh/id_rsa): /home/intelligrape/Do
wnloads/sharad123.pem
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCiBV6Nf7lTHnE10kHhMNQaEyX1TE1cbzILSzqbYUbZ32txSj
zhJ08sv6iGoWT6tThBqIlW4Y+obqLIDtNtYEdFzcESSexrcwT0XHHaDcapqEfpRQNaS0oa4c37xaxq1hCZ+HKw
O58pMYGf0SP9QMtgV53MlTcjecIOD66IGmOspF7FXSPUHiv1Q236zO7EMEaksRIHCShBcAViyca4um4Ma7Pl9Y
AoT4CPgf9dCj0Z/VdAWKWg/2fc4Kzk/PTL4aXsgHUWc67/v9vDVxZYqol+8HhA6epq2YrHQmBKEx2AHBANecQ/
Rs4t+jFyM6f3jW36CP9CPriAxSpcFIntOCoZ
intelligrape@sharad:~$ █
```

The command will ask for the location of private key and will give the public key against that private key on stdout. Copy and save that into a file, with filename "authorized_keys" and put this file inside, '$HOME/chef-repo/cookbooks/changekeypair/files/default/' directory.

```
intelligrape@sharad: ~
intelligrape@sharad:~$ cat chef-repo/cookbooks/changekeypair/files/default/authorized_
keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC8DavahMxKG1Y1R18Petc7RSnQAq+10pwaMkHclGpmbLoQAd
b8KOF6yGGAHHiWPnccDCewkhORwjr5v0xc7GunLL0ifCbkS+fPOF/gAt/eXQ1a2ziQaC7vZ8m+mLQww7ahAJJa
Ok7lWYZFo26coH5Q0SxYPnfajqiVS2l8pHq+I2DQroGUOpZJgTMAuQDSxw88xDTghGWqV5RznhIr72BGJbZ5hn
X02McWtTpQvOYEBDIoUNWgpbxlgk1dIiIc/A7X6vc3P0THVg1xKdZJ8MhcYTSmdfJrCxoSVBG0dwem/IO5vcMD
BIkYeoUiQ0m598BgoWV+KLs0OPb4VkG2Wfut
intelligrape@sharad:~$ █
```

3) Now, we push this public key file inside .ssh folder of all the instances using chef recipe below,

```
intelligrape@sharad: ~
intelligrape@sharad:~$ cat chef-repo/cookbooks/changekeypair/recipes/changekeypair.rb
cookbook_file "/home/ubuntu/.ssh/authorized_keys" do
  source "authorized_keys"
  mode "0600"
end

intelligrape@sharad:~$ █
```

Above recipe will push the "authorized_keys" file to all the chef clients and change its permissions to 600, so that public key held by the clients earlier will be replaced with a new public key. Now users having old private key cannot log into the system.

To add a new user to a server farm with sudo privileges, following steps are to be followed,

1) Create a password shadow hash because original password should not be written in plain text in our recipe.

```
intelligrape@sharad: ~
intelligrape@sharad:~$ openssl passwd -1 "theplaintextpassword"
$1$y8SnSYZo$Yn5yVEeaV6En2VdtzwaNu0
intelligrape@sharad:~$ █
```

2) create a new cookbook and copy the recipe listed below,

```
intelligrape@sharad:~$ cat chef-repo/cookbooks/adduser/recipes/adduser.rb
user 'intelligrape' do
  comment 'user create by Chef recipe'
  home '/home/intelligrape'
  shell '/bin/bash'
  password '$1$RAEc4Buy$.Z7bLGg2wz85rLXpynFOB.'
end

bash 'edit_sudoers' do
  code <<-EOH
    sudo echo 'intelligrape  ALL=(ALL:ALL) ALL' >> /etc/sudoers
  EOH
end
intelligrape@sharad:~$
```

Above recipe will create a new user with username "intelligrape" and password as "theplaintextpassword" and add this user to sudoers.

Thanks and regards
Sharad Aggarwal

Tag -

FOUND THIS USEFUL? SHARE IT

Email   Twitter   Facebook   LinkedIn   Google+

LE

Na

Whitepaper

DevOps Practices and Principles To Improve IT Efficiency

Download Whitepaper (http://insights.tothenew.com/devops-practices-principles-for-it-efficiency)

by

Sharad Aggarwal (http://www.tothenew.com/blog/author/sharadaintelligrape-com/)

YOU MAY ALSO LIKE

Chef recipe to deploy Grails war on a new production server (http://www.tothenew.com/blog/chef-recipe-to-deploy-grails-war-on-a-new-production-server/)

Puppet manifests to change pem key of running ec2 instances (http://www.tothenew.com/blog/puppet-manifests-to-change-pem-key-of-running-ec2-instances-and-adding-a-new-user-to-all-the-instances-and-give-sudo-privileges/)

Register chef-client in AWS Autoscaling (http://www.tothenew.com/blog/register-chef-client-in-aws-autoscaling/)

FOLLOW US ON

(https://www.facebook.com/TOTHENEWhttps://twitter.com/totalgravitytohttps://linkedin.com/company/tothenew)

Subscribe to our Blog

Get latest articles straight to your inbox

ENTER EMAIL | Subscribe Now

Who We Are   +

What We Do   +