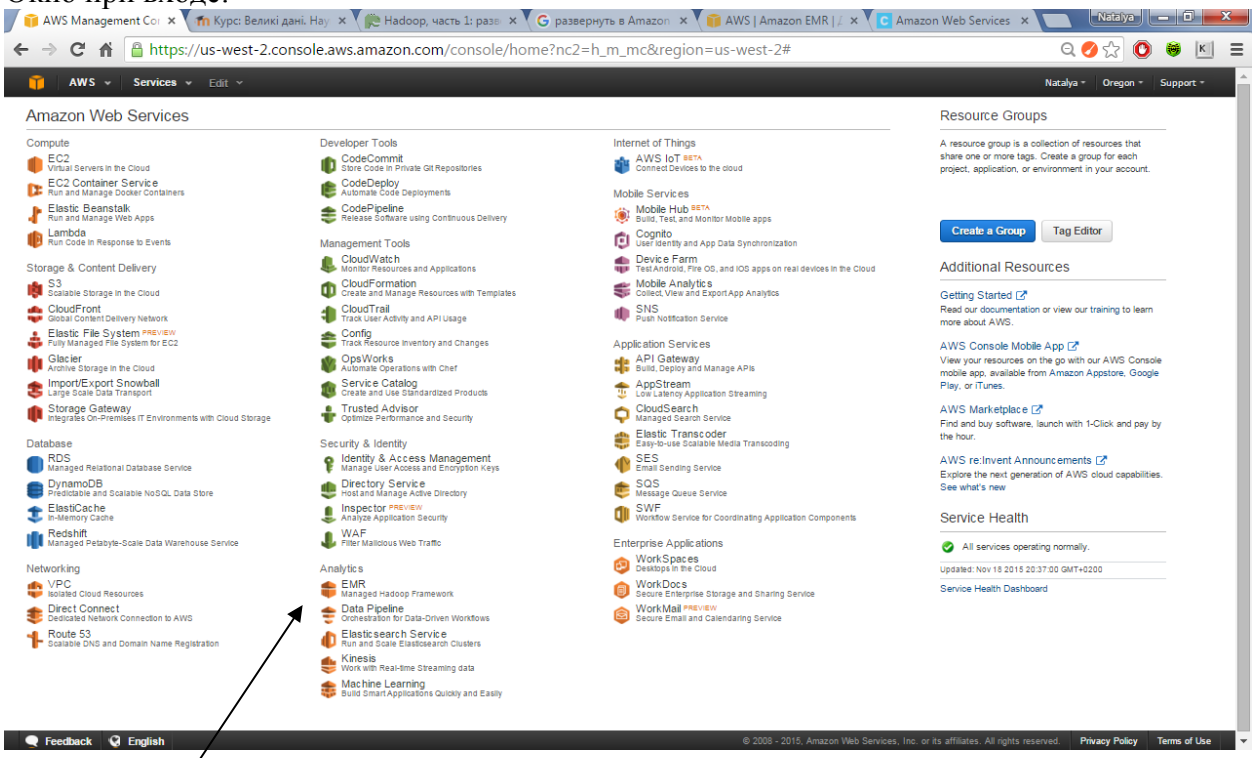
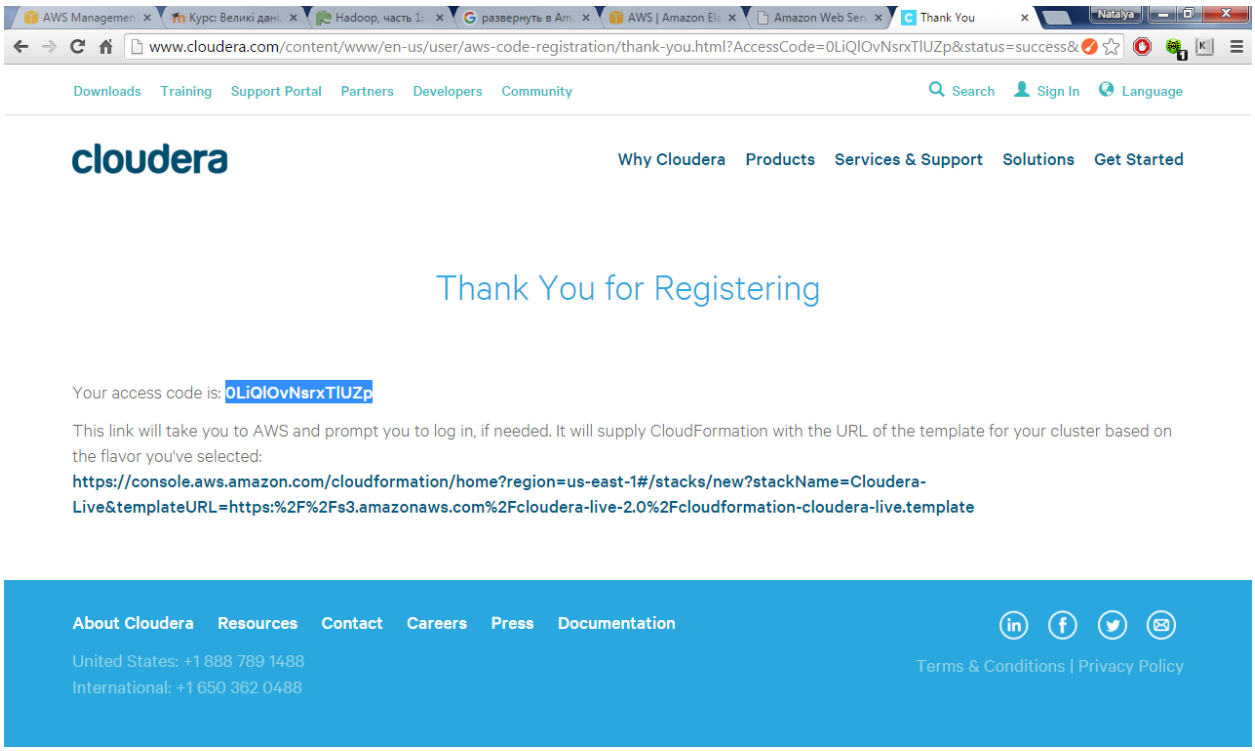
Итак, AWS свободный аккаунт создан.
Окно при входе:



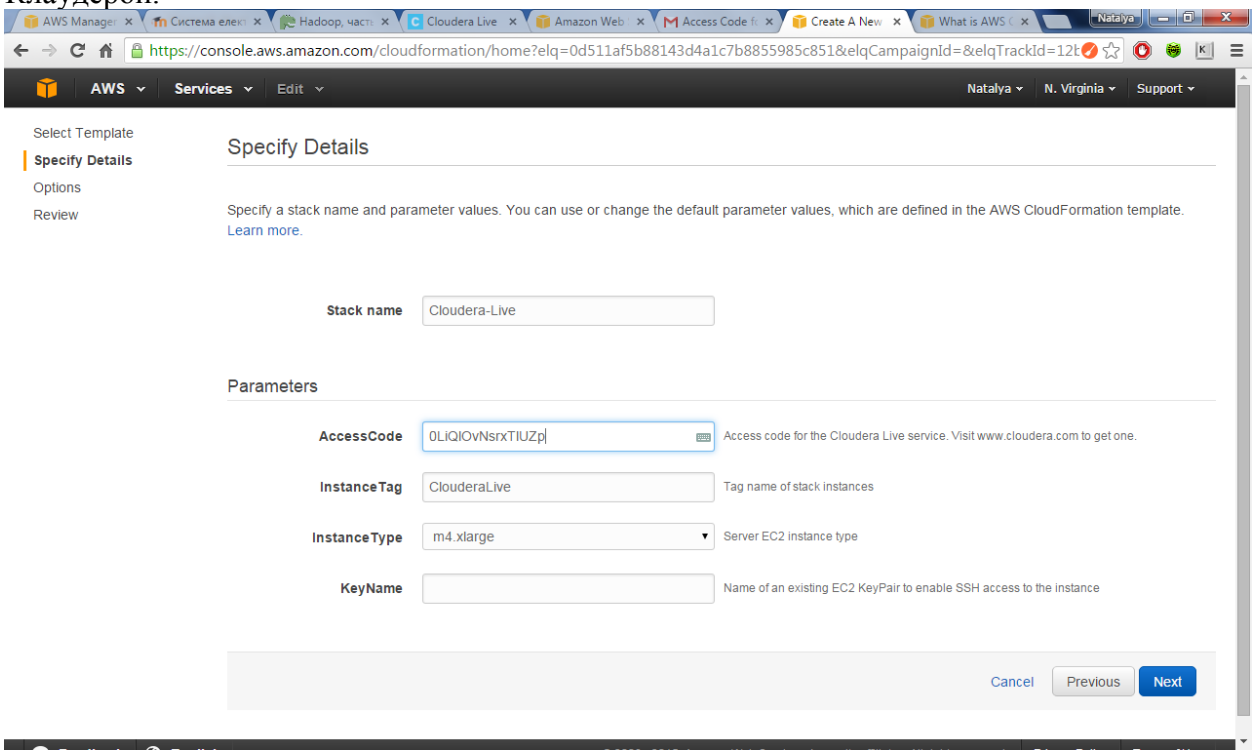
Elastic Map Reduce (EMR) - $40/месяц

Альтернатива:Cloudera Live Tutorials на Cloudera Enterprise
http://www.cloudera.com/content/www/en-us/developers/get-started-with-hadoop-tutorial.html
Что там нужно ставить – см тьюториал:
http://www.cloudera.com/content/www/en-us/developers/get-started-with-hadoop-tutorial/setup.html
Быстро регистрируемся и получаем код и страницу доступа:



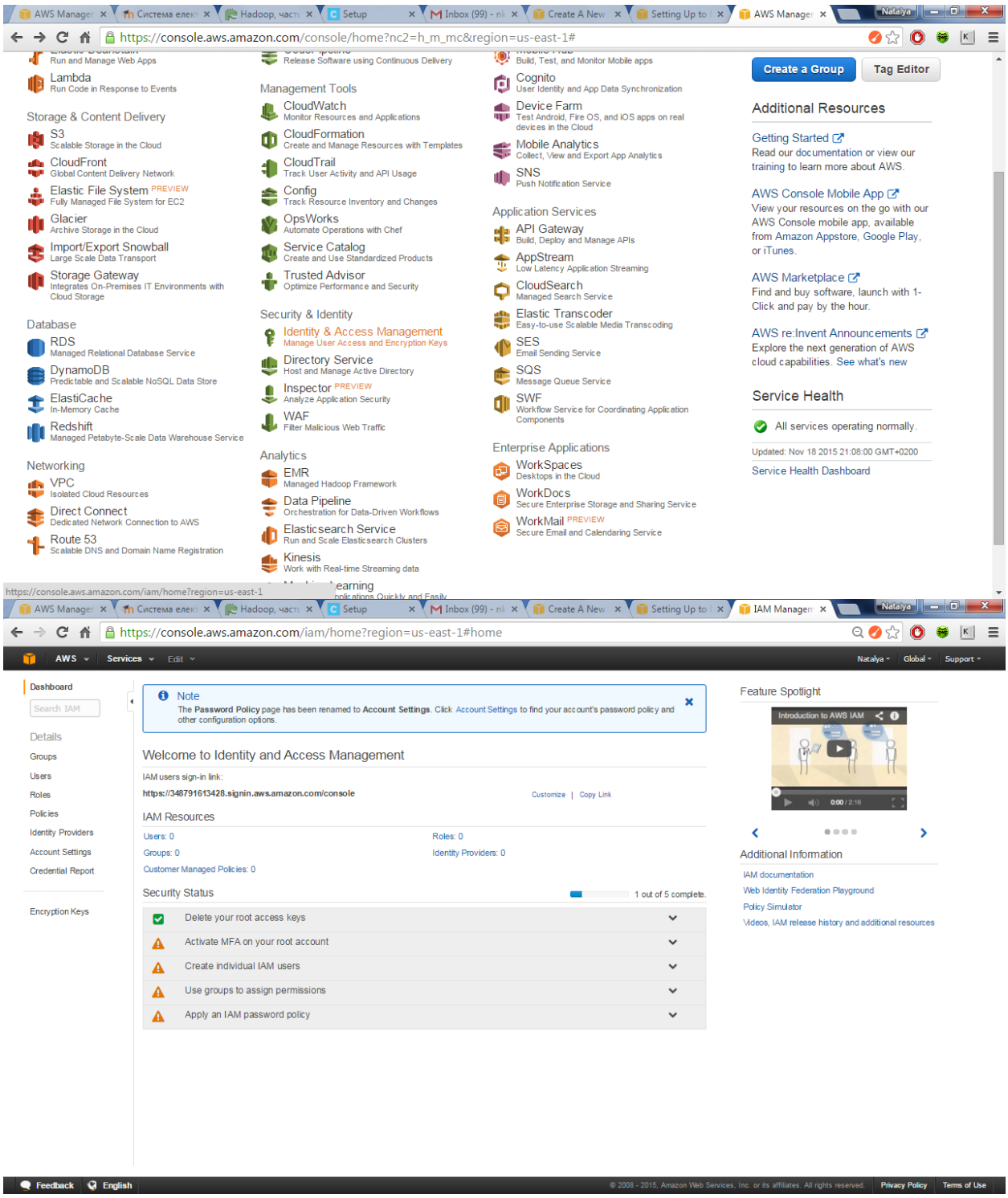
Первый шаг: выбор конфигурации облака. Главный принцип – остаться в рамках бесплатного плана AWS. Пропускаем его.

Второй шаг – детали Cloudera Live tutorial. Вводим ключ из письма,присланного Клаудерой.



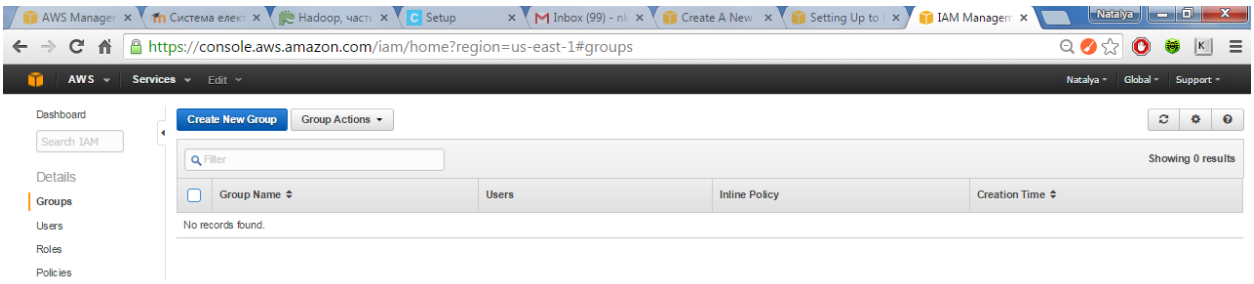
Тут требуется ключ KeyName. Следует его создать в консоли AWS.

Инструкции – здесь: http://docs.aws.amazon.com/gettingstarted/latest/wah/getting-started-prereq.html

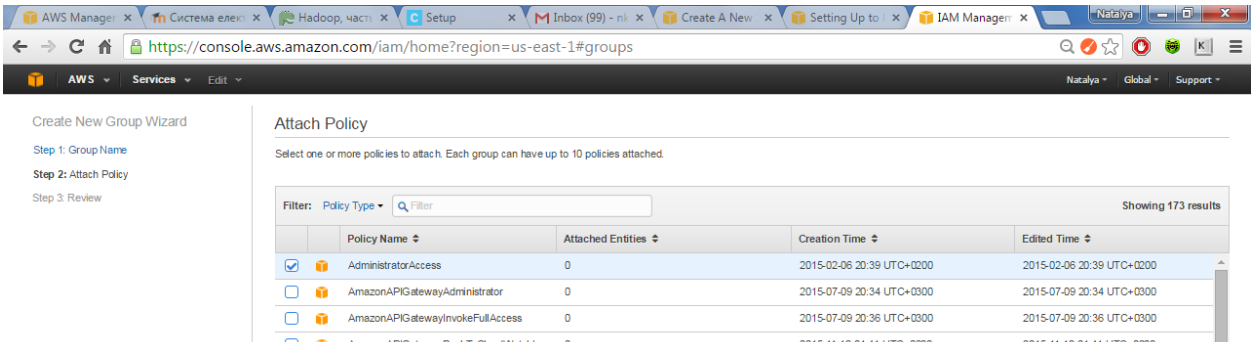


To create a group for administrators

1. Sign in to the AWS Management Console and open the IAM console athttps://console.aws.amazon.com/iam/.
2. In the navigation pane, choose **Groups**, and then choose **Create New Group**.



3. For **Group Name**, type a name for your group, such as `Administrators`, and then choose **Next Step**.
4. In the list of policies, select the check box next to the **AdministratorAccess** policy. You can use the **Filter**menu and the **Search** box to filter the list of policies.

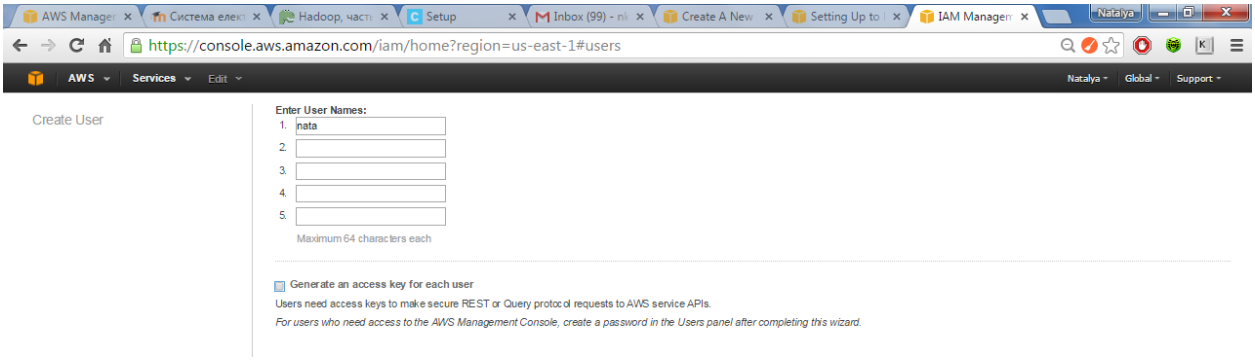


5. Choose **Next Step**, and then choose **Create Group**.

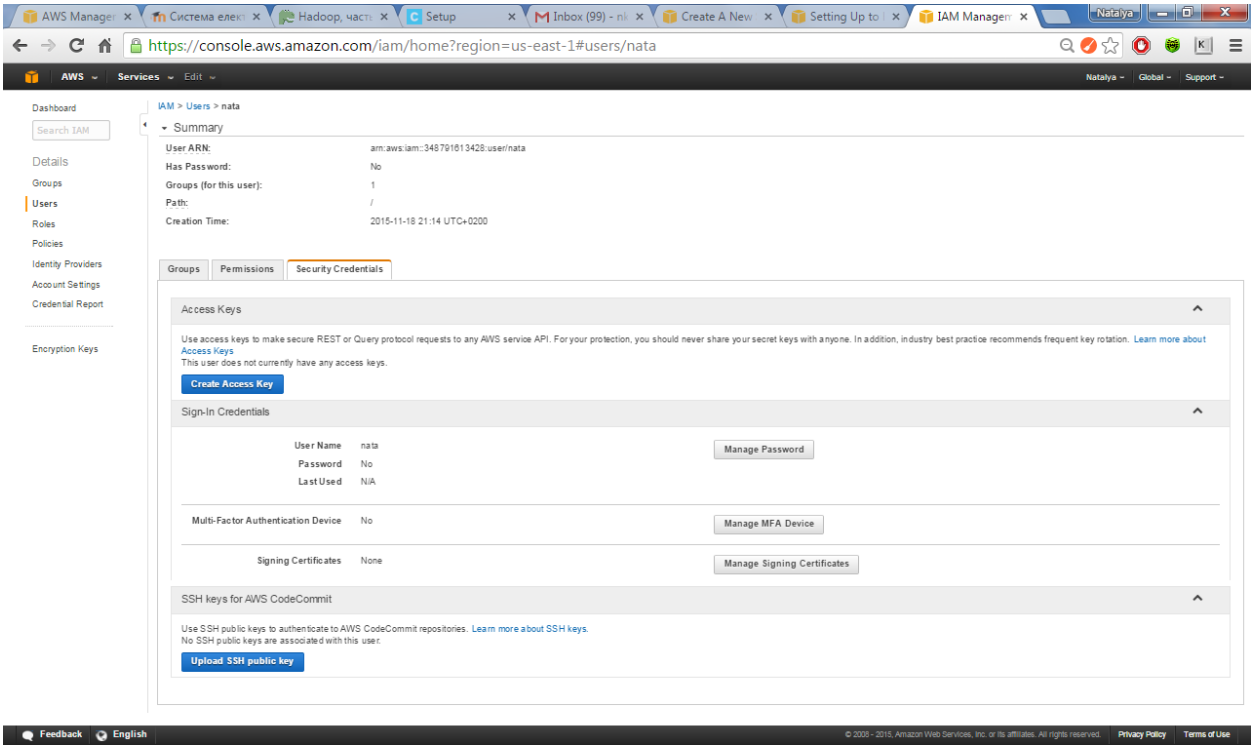
Your new group is listed under **Group Name**.

To create an IAM user for yourself, add the user to the administrators group, and create a password for the user

1. In the navigation pane, choose **Users**, and then choose **Create New Users**.
2. In box **1**, type a user name. Clear the check box next to **Generate an access key for each user**. Then choose **Create**.
3.



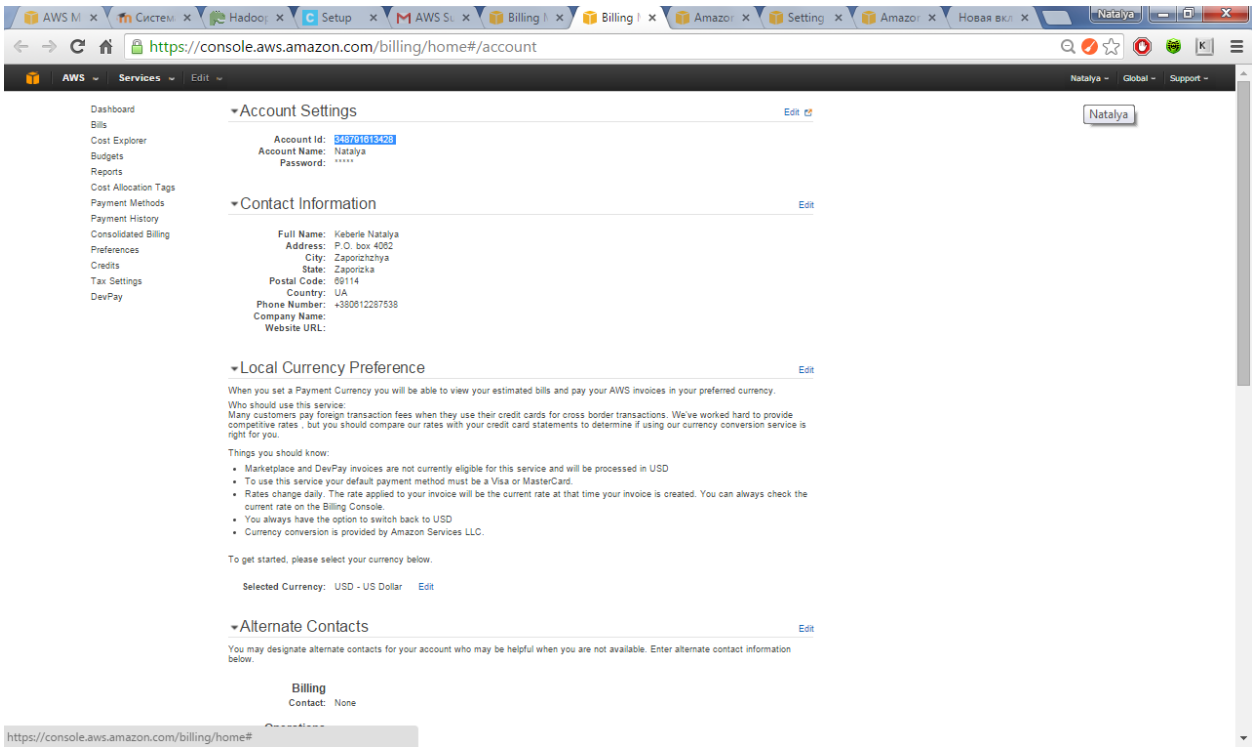
4. In the list of users, choose the name (not the check box) of the user you just created. You can use the **Search** box to search for the user name.
5. Choose the **Groups** tab and then choose **Add User to Groups**.
6. Select the check box next to the administrators group. Then choose **Add to Groups**.
7. Choose the **Security Credentials** tab. Under **Sign-In Credentials**, choose **Manage Password**.



8. Select **Assign a custom password**. Then type a password in the **Password** and **Confirm Password** boxes. When you are finished, choose **Apply**.

Пароль **4nata**

Далее, можно не выходя, узнать через профиль аккаунт



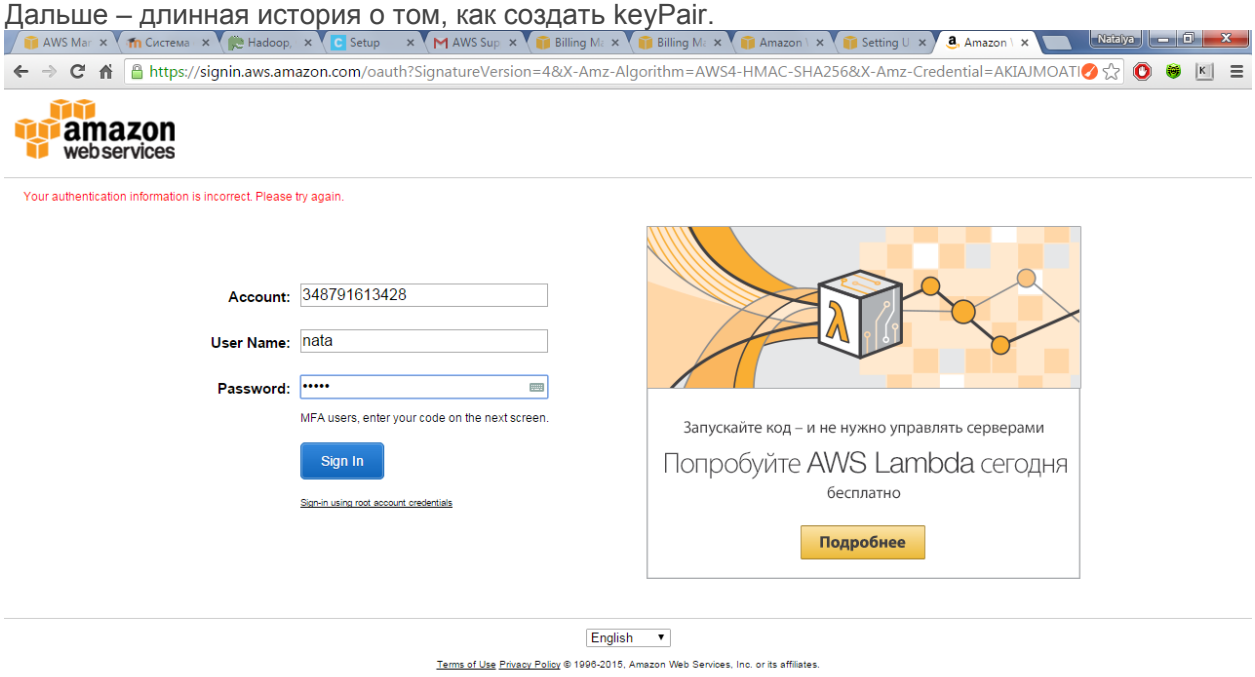
348791613428

И зайти с адреса: https://your_aws_account_id.signin.aws.amazon.com/console/

где your_aws_account_id=348791613428

в консоль. Вводим имя пользователя и пароль, только что созданные в IAM.

Дальше – длинная история о том, как создать keyPair.



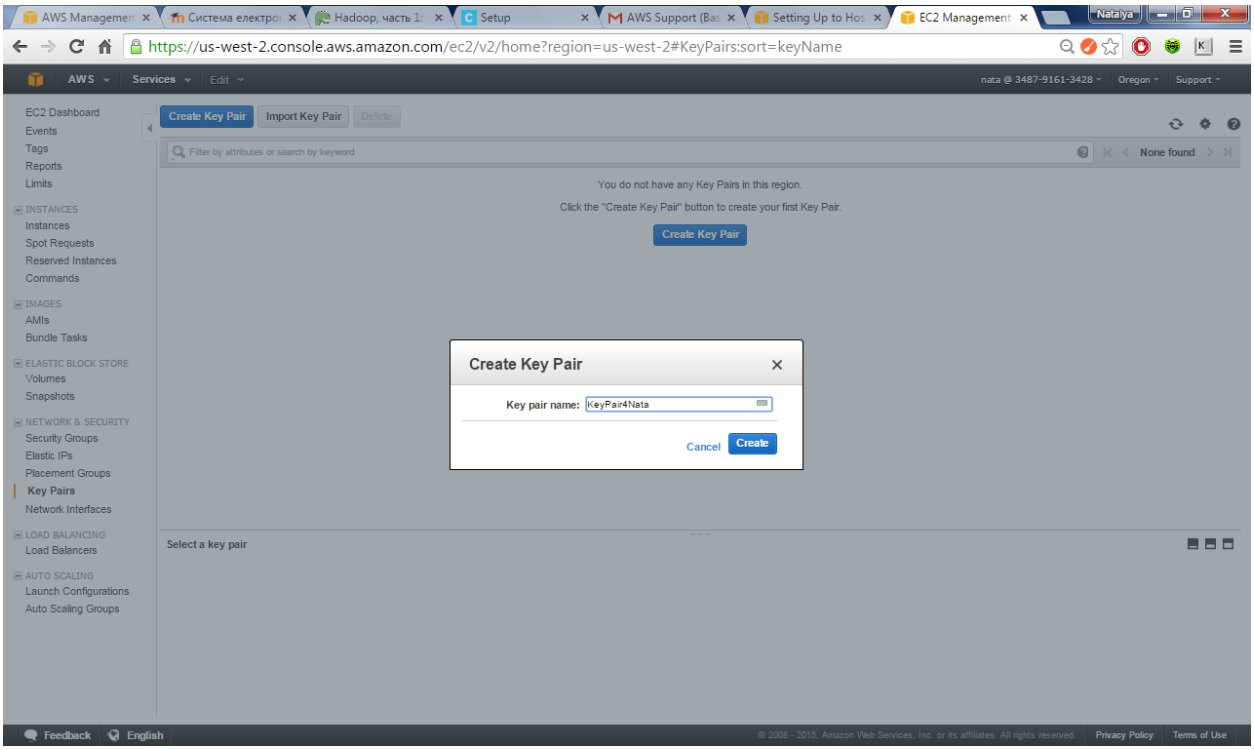
Create a Key Pair

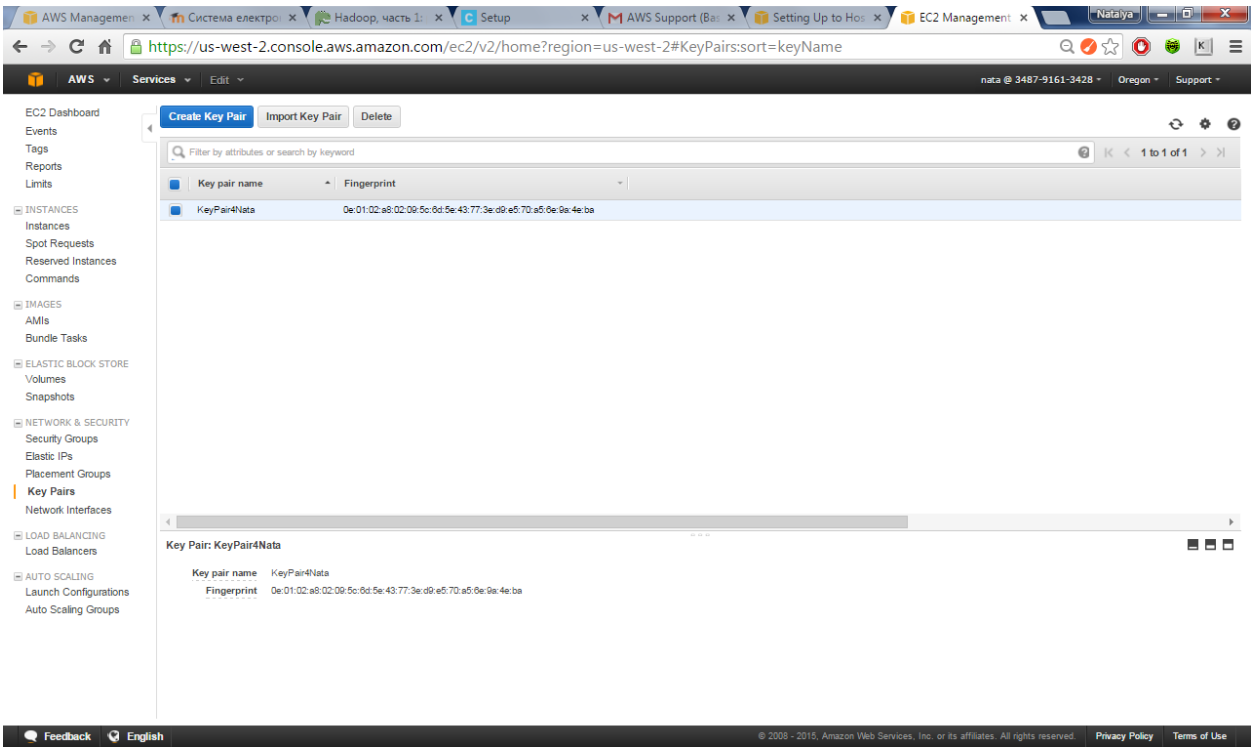
AWS uses public-key cryptography to secure the login information for your instance. You specify the name of the key pair when you launch your instance, then provide the private key to obtain the administrator password for your Windows instance so you can log in using RDP.

If you haven't created a key pair already, you can create one using the Amazon EC2 console.

To create a key pair

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. From the navigation bar, in the region selector, click **US West (Oregon)**.
3. In the navigation pane, click **Key Pairs**.
4. Click **Create Key Pair**.
5. Enter a name for the new key pair in the **Key pair name** field of the **Create Key Pair** dialog box, and then click **Create**. Choose a name that is easy for you to remember.





6. The private key file is automatically downloaded by your browser. The base file name is the name you specified as the name of your key pair, and the file name extension is `.pem`. Save the private key file in a safe place.

   Important

   This is the only chance for you to save the private key file. You'll need to provide the name of your key pair when you launch an instance and the corresponding private key each time you connect to the instance.

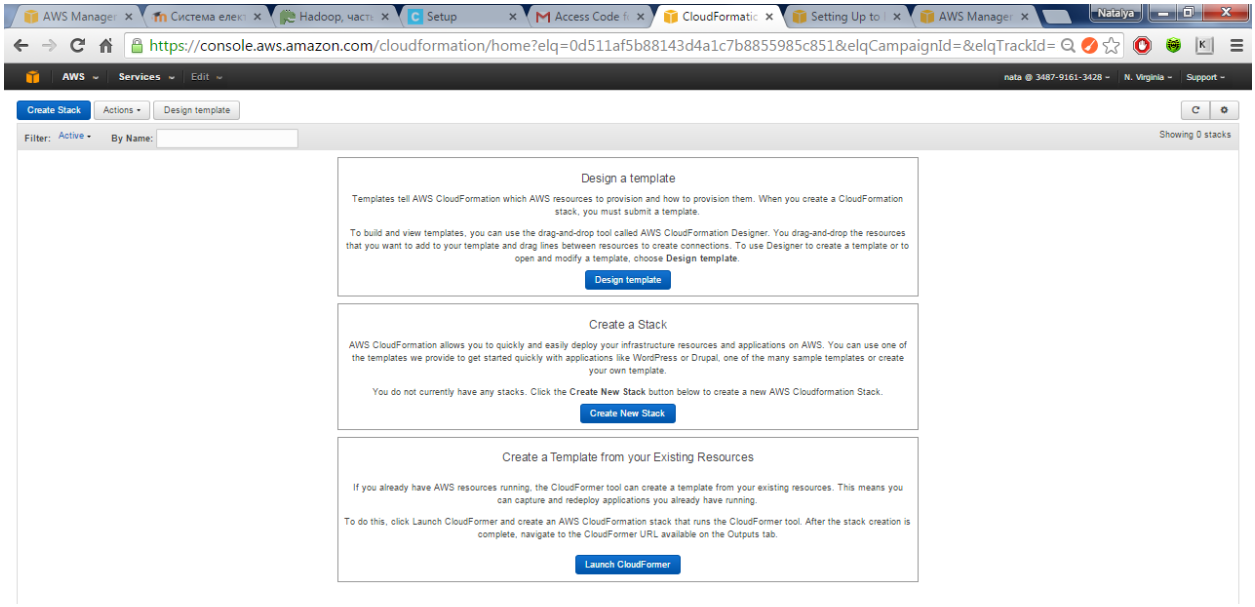
7. Prepare the private key file. This process depends on the operating system of the computer that you're using.
   - If your computer runs Mac OS X or Linux, use the following command to set the permissions of your private key file so that only you can read it.

     ```
     $ chmod 400 my-key-pair.pem
     ```

   - If your computer runs Windows, use the following steps to convert your .pem file to a .ppk file for use with PuTTY.
     a. Download and install PuTTY from http://www.chiark.greenend.org.uk/~sgtatham/putty/. Be sure to install the entire suite.
     b. Start PuTTYgen (for example, from the **Start** menu, click **All Programs > PuTTY > PuTTYgen**).
     c. Under **Type of key to generate**, select **SSH-2 RSA**.

d. Click **Load**. By default, PuTTYgen displays only files with the extension `.ppk`. To locate your `.pem`file, select the option to display files of all types.
e. Select your private key file and then click **Open**. Click **OK** to dismiss the confirmation dialog box.
f. Click **Save private key**. PuTTYgen displays a warning about saving the key without a passphrase. Click **Yes**.
g. Specify the same name that you used for the key pair (for example, *`my-key-pair`*) and then click**Save**. PuTTY automatically adds the `.ppk` file extension.

после всех усилий получаем созданное для CLoudera облако в AWS



Правильный ответ: сервис в процессе создания