Preparing for Splice Machine on Your AWS Account

Splice Machine needs a little information from you to help us configure our service on your AWS account; please fill in the fields in this document so we can get you set up.

We need you to complete these steps, each of which is detailed in a section below:

1. Configure a User Policy	One of your users who has programmatic access to AWS needs to have a specific IAM policy configuration.
2. Provide a Key Pair PEM File	We need a PEM file for an AWS Key Pair we can use to set up your environment.
3. Provide an ARN for Your SSL Certificate	You'll need a wildcard SSL certificate for your domain, and we'll the Amazon Resource Name (*ARN*) for that certificate.
4. Provide Your AWS Account ID	We need this to share our Amazon Machine Images (*AMI*s) with your account.
5. Specify Values for Infrastructure Properties	Please provide values for the infrastructure properties listed in this section.
6. Specify Property Values for Your Application Environment	We also need you to supply a few application-specific property values, which are listed in this section.

1. Configure a User Policy

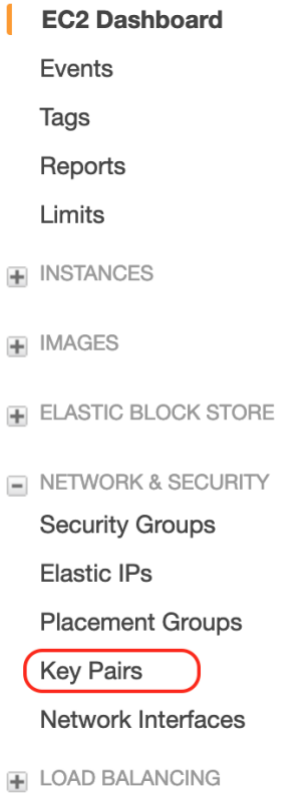
One of your users who has programmatic access to AWS needs to have the following IAM policy configuration:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "autoscaling:*",
        "ec2:*",
        "elasticloadbalancing:*",
        "es:*",
        "iam:AddRoleToInstanceProfile",
        "iam:AttachRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:CreatePolicy",
        "iam:CreateRole",
        "iam:CreateServiceLinkedRole",
        "iam:DeleteRole",
        "iam:DetachRolePolicy",
        "iam:GetInstanceProfile",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetUserPolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfilesForRole",
        "iam:ListPolicyVersions",
        "iam:ListPolicyVersions",
        "iam:PassRole",
        "rds:*",
        "route53:*",
        "s3:*",
        "tag:*"
      ],
      "Resource": "*"
    }
  ]
}
```

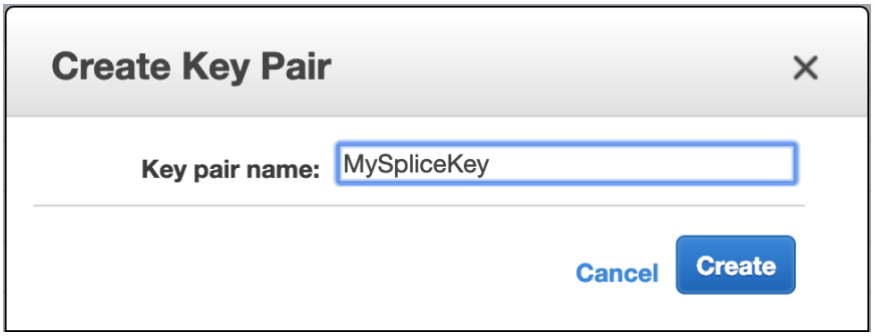
2. Provide a Key Pair PEM File

To set up your environment, Splice Machine needs the PEM file for an Amazon Key Pair. If you don't yet have a Key Pair, you can create one as follows:

1. Log into the *AWS Console* and navigate to EC2 from the navigation pane; or point your browser at https://console.aws.amazon.com/ec2/
2. In the navigation pane on the left side of the console, select *Key Pairs*, which is under *NETWORK & SECURITY*:



3. Select *Create Key Pair* at the top of the window.
4. Enter a name for the new key pair and select *Create*:



5. AWS creates your key pair and downloads the private key (**keyname.pem**) file to your computer. Save this key file in a safe location.
6. Use the following command to modify the permissions on the PEM file:

   chmod 600 *path/to/file/keyname*.pem

7. Now move the PEM file:

   cp *path/to/file/keyname*.pem ~/.ssh

8. And finally, add it to ssh:

   ssh add ~/.ssh/*keyname*.pem

For more information about creating and using key pairs, see:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html

3. Provide an ARN for Your SSL Certificate

You need to provision an SSL certificate domain you're using for Splice Machine, and we need the Amazon Resource Name (*ARN*) for that certificate.

You can follow these steps to create the certificate if you don't already have one for the domain:

1. Log into the *AWS Console* and navigate to the Certificate Manager from the navigation pane; or point your browser https://console.aws.amazon.com/acm/home.
2. Select *Provision certificates*.
3. Select the *Request a public certificate* radio button.
4. Click *Request a Certificate*.
5. Specify a domain name with a wildcard; for example:

   ***.splicemachine-test.io**

6. Click the *Next* button.
7. Follow the instructions on AWS for validating the certificate through DNS or e-mail.

4. Provide Your AWS Account ID

We need to share our AMIs with the Customer's AWS Account. In order to do that we need the AWS Account Id:

Your AWS Account ID:	

5. Specify Values for Infrastructure Properties

Please fill in your values for the following infrastructure properties.:

	Name and Description	Enter Your Value
1.	*AWS Region* Enter the AWS region to use. Choose from: • us-east-1 • us-east-2 • us-west-1 • us-west-2	us-east-1
2.	*AWS SSL Certificate ARN* Provide the ARN for the certificate (see step 3, above)	
3.	*CIDR Block* Specify a range of IPv4 addresses for the Virtual Private Cloud (*VPC*) in a Classless Inter-Domain Routing (CIDR) block. For example: 10.0.0.0/16	
4.	*Key Name* The name of the key pair use to ssh into the machines. This name must be shown in the *Network & Security-> Key Pairs* section of the EC2 Manager. (see step 2, above)	
5.	*Instance Types* Specify the type of EC2 instance to use for each server type. The default values are:	*HDD* d2.xlarge *MASTER* m4.4xlarge *PRIVATE AGENT* m4.4xlarge *PUBLIC AGENT* m4.large *SPARK* i3.4xlarge
6.	*Instance Type Root Size* Specify the root size to use for each server type. The default values are:	*HDD* 300 *MASTER* 300 *PRIVATE AGENT* 300 *PUBLIC AGENT* 300 *SPARK* 300

	Name and Description	Enter Your Value
7.	*Instance Counts* Specify the required number of instances for each instance type:	*HDD* 4 *MASTER* 3 *PRIVATE AGENT* 6 *PUBLIC AGENT* 3 *SPARK* 4
8.	*Metadata Database Name* The name of the Postgres database used to store the metadata for the Cloud Manager	
9.	*Metadata Database User Name* The username for the Postgres database	
10.	*Metadata Database Password* The password for the Postgres database	
11.	*Elasticsearch Domain* The name of the domain used for the elasticsearch instance	
12.	*Elasticsearch Instance Type* The instance type for elasticsearch; the default value is m4.large.elasticsearch.	m4.large.elasticsearch
13.	*Elasticsearch Instance Count* The number of elasticsearch instances to use. The default value is 4.	4
14.	*Elasticsearch EBS Volume Size* The size of the EBS volume. The default value is 300.	300
15.	*Spark Temp Space Disk Size* The size of the spark temporary space. The default value is 1000GB.	1000
16.	*VPC CIDR Block* The CIDR block to use when creating the IP addresses for your instances.	

	Name and Description	Enter Your Value
17.	*Cluster Tags* The tags to use on all of your cluster resources for identification and billing purposes.	*Cluster Name* *Dept Name* *Resource Owner* *Resource Purpose*
18.	*Whitelist IP Addresses* IP addresses to add for limiting access to DCOS admin components.	
19.	*Zone* The domain name for the database instance URLs.	
20.	*Environment* The environment suffix to add to each URL; one of: • dev • qa • *(none)* The default value is none (no suffix)	

6. Specify Property Values for Your Application Environment

Finally, please provide the following information for setting up your application environment:

	Name and Description	Enter Your Value
1.	*Auth0 certifcate*	
2.	*Auth0 client ID*	
3.	*Auth0 domain*	
4.	*BCC Email address* This is the address to which the cluster creation email should be sent.	

	Name and Description	Enter Your Value
5.	*Google Analytics tracking ID* (optional)	
6.	*SMTP e-mail properties*	*Host:* *Password:* *Port:* *User ID:*