Manual AWS Deployment

This document assumes you are familiar with the AWS console and can navigate and create resources there.

The high level tasks are:

- Create AWS Key-pair
- Create Policies and Roles
- Create VPC, subnets, Internet Gateway, NAT Gateway, Security Groups
- Create a Launch Configuration
- Create an Auto-scale Group
- Create an EC2 instance for the installer
- Setup MapR installer
- Create AWS credentials file

Create AWS Key-pair

See http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html) on creating key-pairs

Create Policies and Roles

If there are restriction in creating roles and policies, you can add the AWS API credentials on the installer node. See section on “Setup the Installer”

There is cloud-formation template that can create these for you: Launch Stack (https://console.aws.amazon.com/cloudformation/home?region=us-east-2#/stacks/new?templateURL=https://s3.us-east-2.amazonaws.com/mapr-installer/templates/aws/aws_cf_maprcluster_vpc.yml)

Otherwise, follow these steps:

1. Create Policy The policy statement would be:

```
{
       "Version": "2012-10-17",
       "Statement": [
           {
               "Effect": "Allow",
               "Action": [
                   "autoscaling:Describe*",
                   "autoscaling:CreateLaunchConfiguration",
                   "autoscaling:DeleteLaunchConfiguration",
                   "autoscaling:SuspendProcesses",
                   "autoscaling:UpdateAutoScalingGroup",
                   "cloudformation:DescribeStack*",
                   "cloudformation:GetTemplate",
                   "cloudformation:UpdateStack",
                   "ec2:CreateKeyPair",
                   "ec2:DeleteKeyPair",
                   "ec2:ImportKeyPair",
                   "ec2:DescribeKeyPairs",
                   "ec2:DescribeInstances",
                   "ec2:DescribeInstanceAttribute",
                   "ec2:ModifyInstanceAttribute",
                   "ec2:DescribeSubnets",
                   "ec2:RunInstances",
                   "ec2:StartInstances",
                   "ec2:StopInstances",
                   "ec2:CreateVolume",
                   "ec2:AttachVolume",
                   "ec2:DescribeVolumes"
               ],
               "Resource": "\*"
           }
       ]
   }
```

2. Create Role with the policy created above.

Note: You as a user must have the IAM:PassRole permission

Create VPC, subnets, Internet Gateway, NAT Gateway, Security Groups

You can use an existing VPC if that satisfies the following requirements:

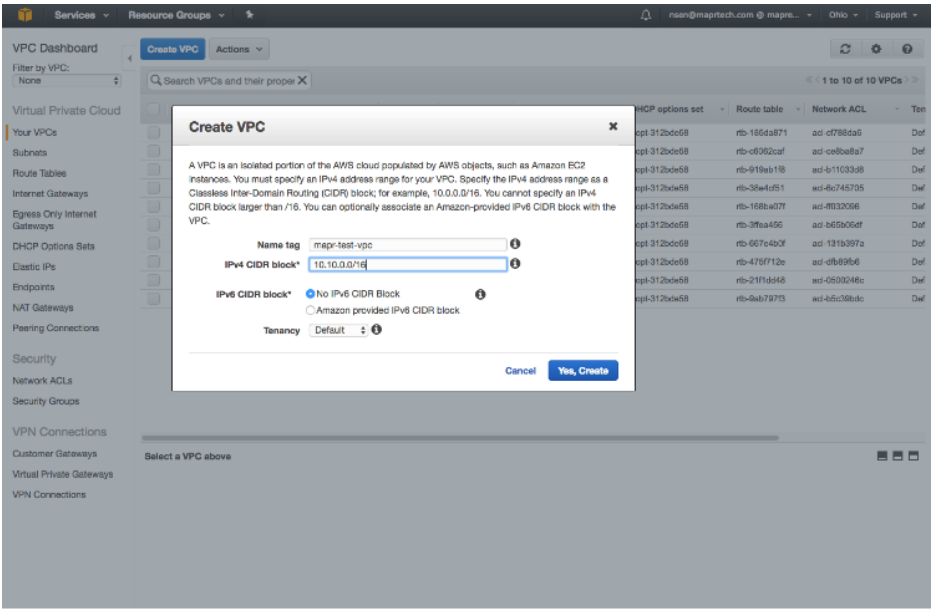
- Instances can be created in a subnet that can talk to the Internet (to download MapR packages)

- Instances can talk to each other within the VPC

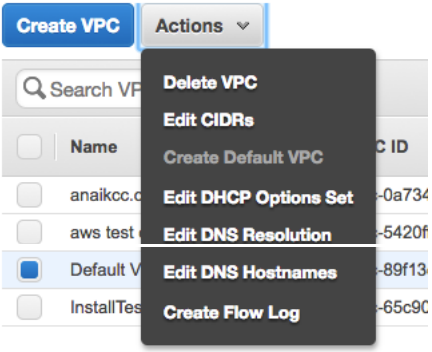
Otherwise, follow these steps:

1. Create VPC
    1. Make sure that "DNS Resolution" and "DNS Hostnames" are enabled for the VPC
2. Create two subnets These will be configured such that one can be accessed from the Internet (public-subnet), another can talk to the Internet but cannot be accessed from outside (private-subnet)
3. Create Internet Gateway
4. Attach Internet Gateway to the VPC
5. Create Elastic IP
6. Create NAT Gateway - attach it to the public subnet
7. Update default Route Table for VPC to allow Internet access via Internet Gateway
8. Create a new Route
    1. Update the route to allow the private-subnet to talk to the Internet via NAT Gateway
    2. Associate private subnet to the new route
9. Create Security groups
    1. SSH Access
        1. Ports: 22
    2. Web Access
        1. Ports: 9443, 8443, 8042, 8047, 8088, 8888, 18080, 19888

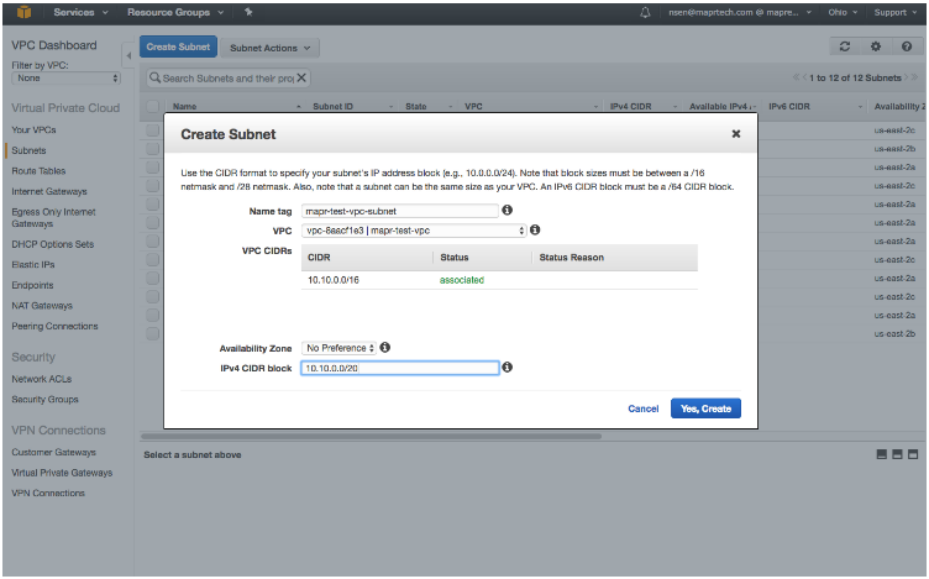
Create VPC



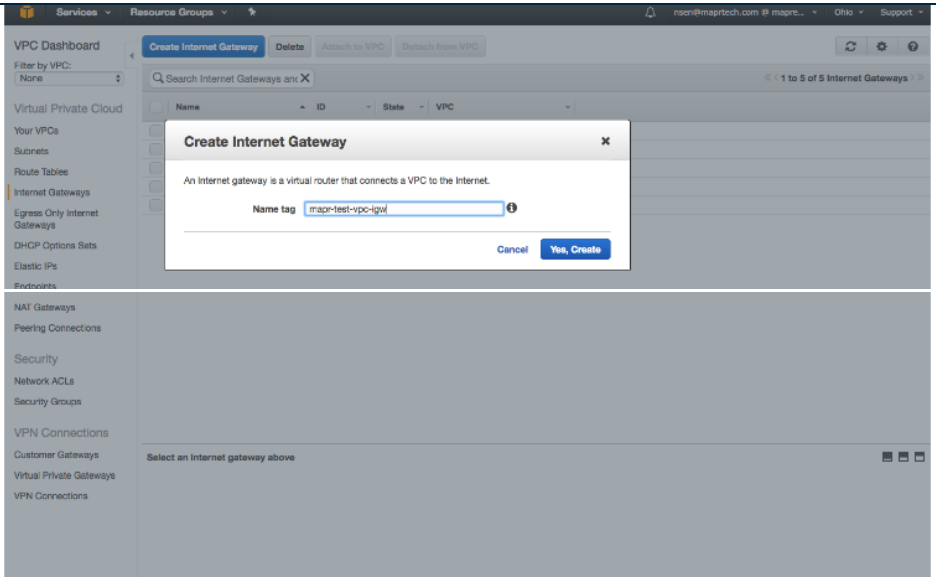
DNS Resolution and DNS Hostnames are enabled



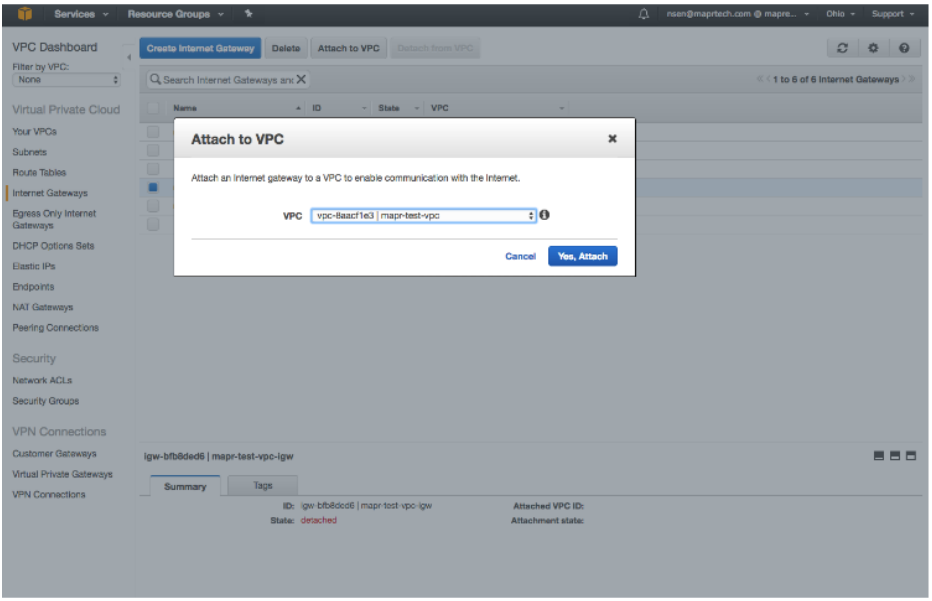
Create two subnets in the VPC you created above (you need to do this step twice - once for each subnet). The subnet CIDR should be different and non-overlapping for the two subnets. So, if your VPC CIDR is 10.10.0.0/16, your public subnet CIDR could be 10.10.0.0/24 and private subnet CIDR could be 10.10.8.0/22



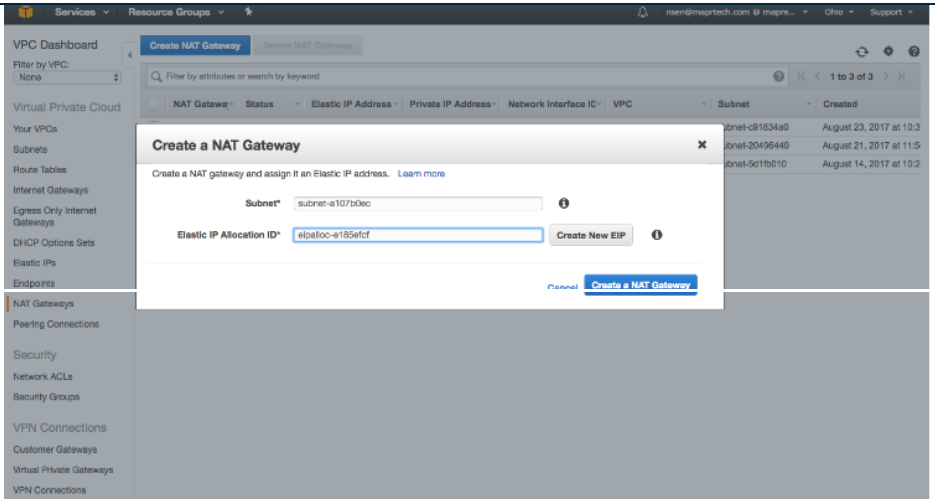
Create Internet Gateway



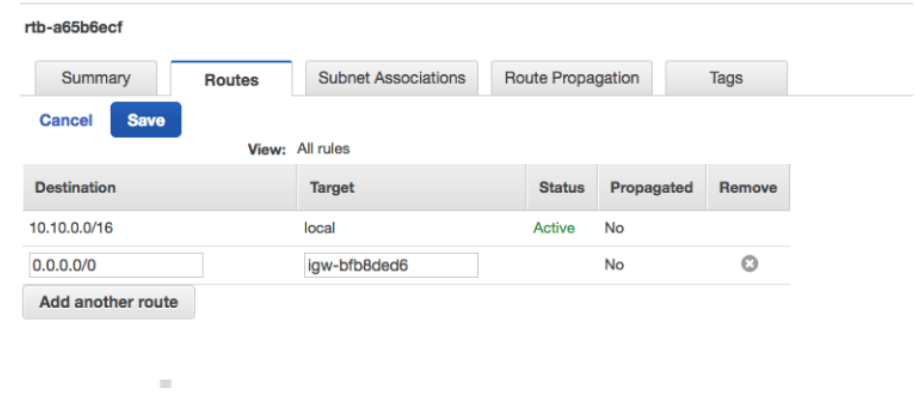
Attach Internet Gateway to VPC



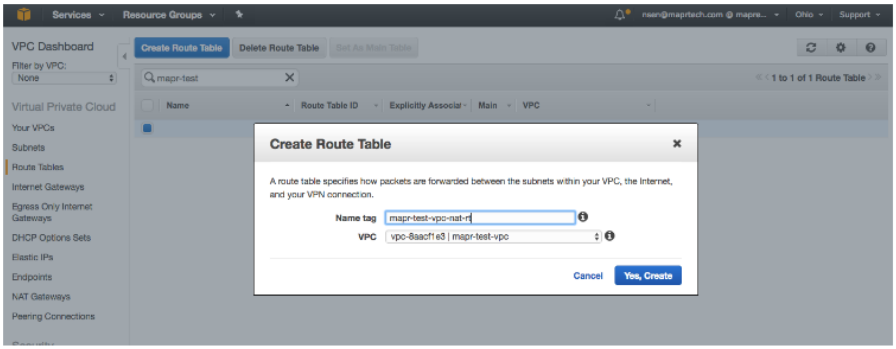
Create NAT Gateway - choose the public subnet



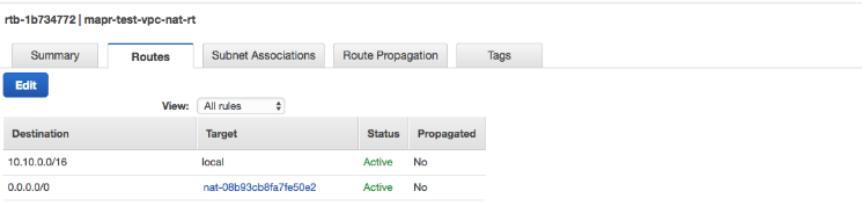
Update default route table for VPC to route all trafic to Internet Gateway



Create a new route table for private subnet

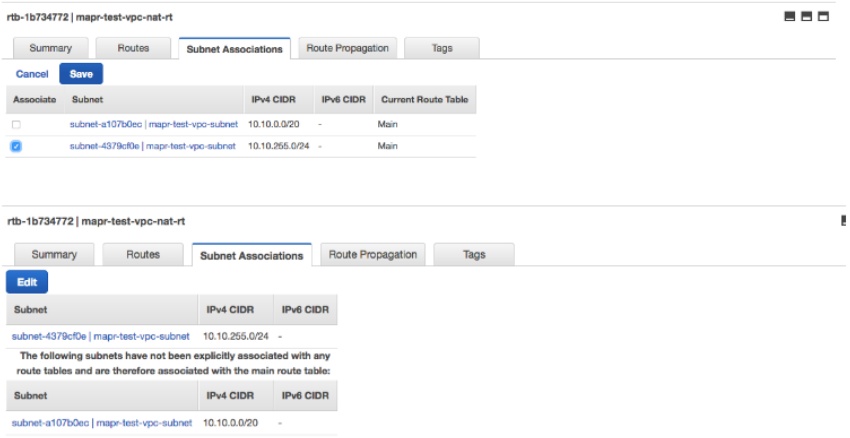


Update the route table to route all traffic to the NAT gateway

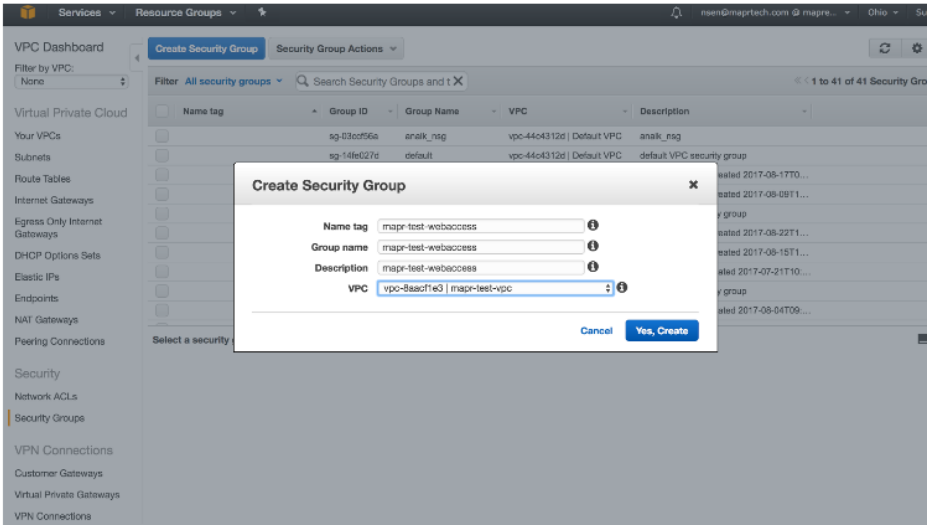


Associate route table with the private subnet

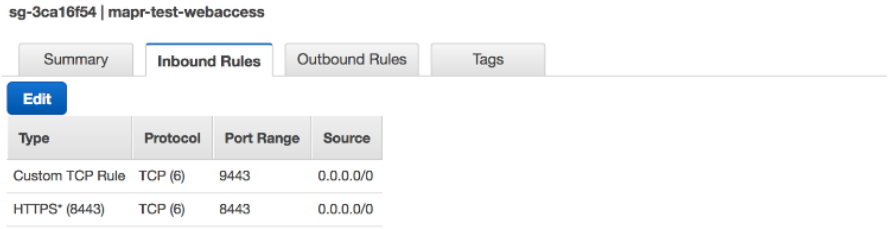
Associate route table with the private subnet



Create Security Groups



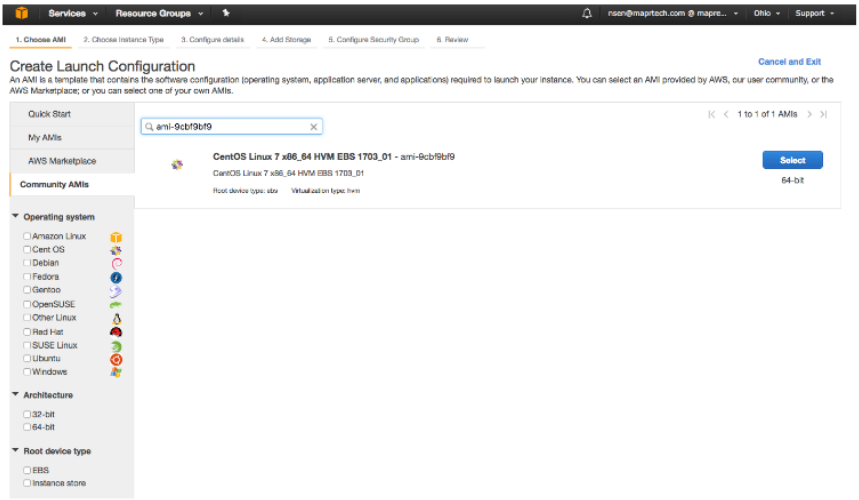
Add Inbound security rules

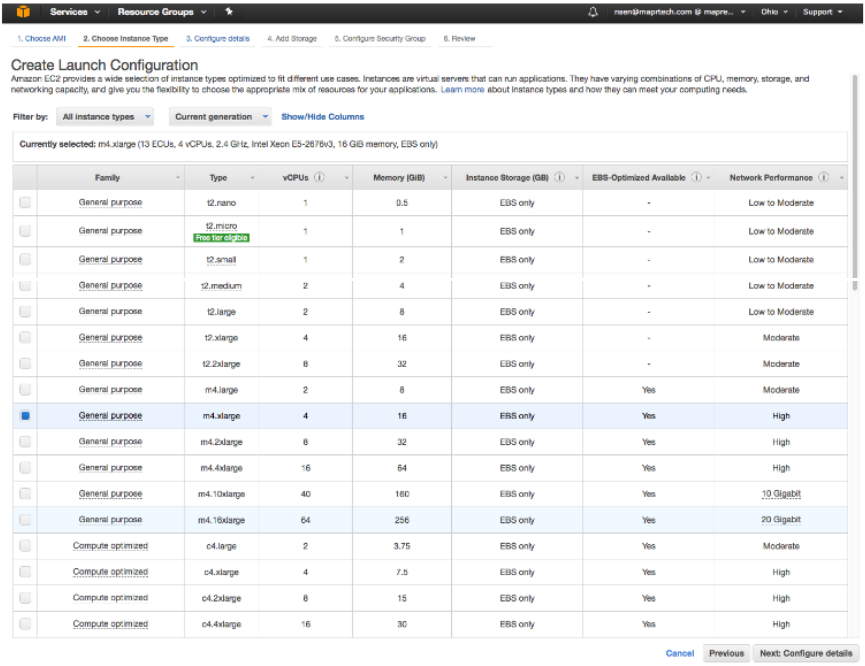


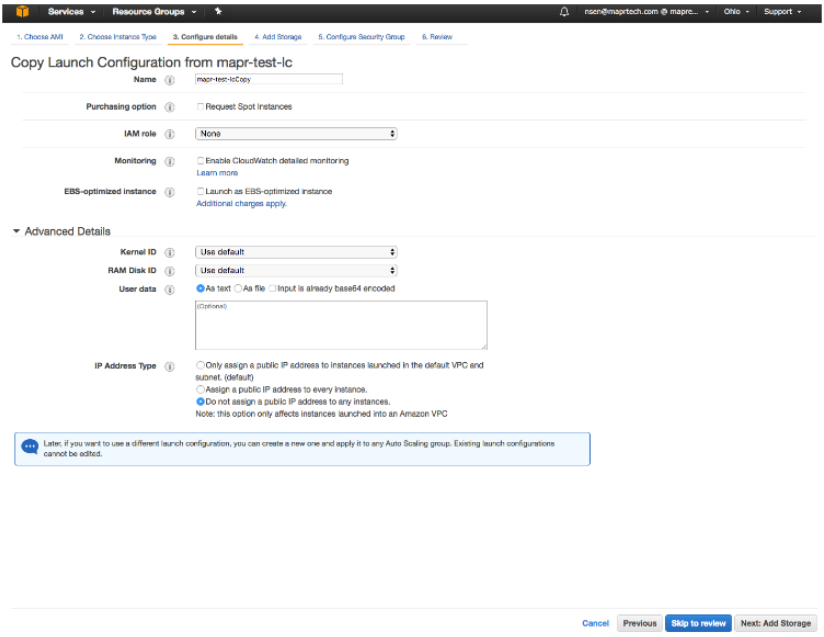
Create a Launch Configuration

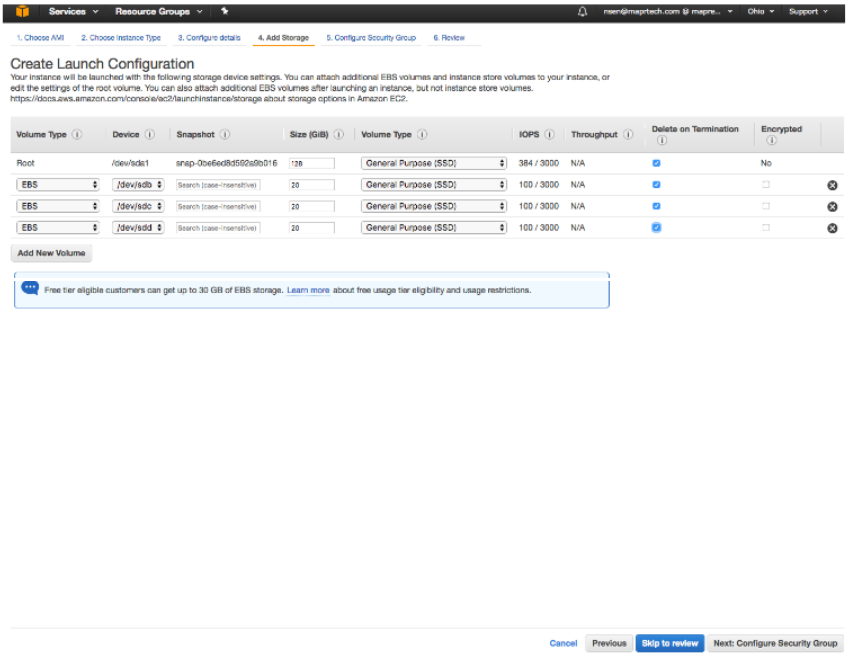
From AWS console, create launch configuration:

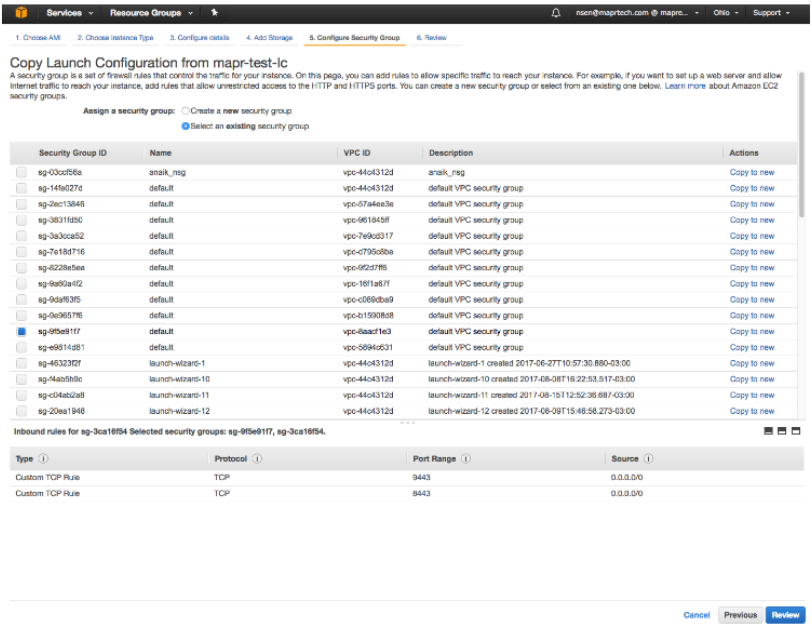
- Choose AMI
- Choose machine type
- Provide launch configuration name
  - Choose either the 2nd or 3rd option for IP Address Type under Advanced options
- Add storage
  - Increase the root disk size to minimum of 128G
  - Add as many disks, along with their size, for data disks on the nodes
- Select security groups
  - The default security group for the VPC that will allow the instances to talk to each other
  - The security group created to allow web access to the MapR services
- Select the AWS Keypair to be used

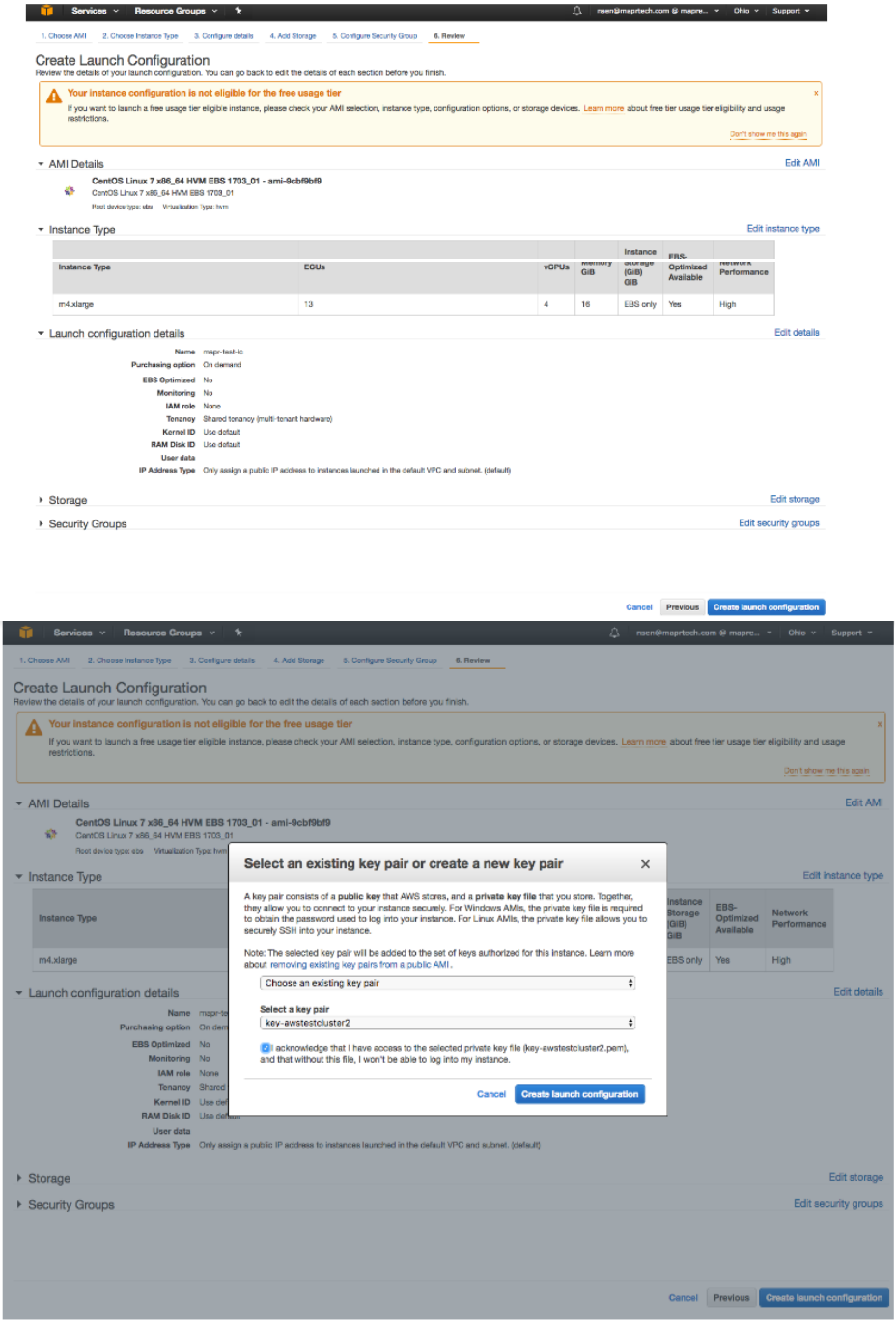


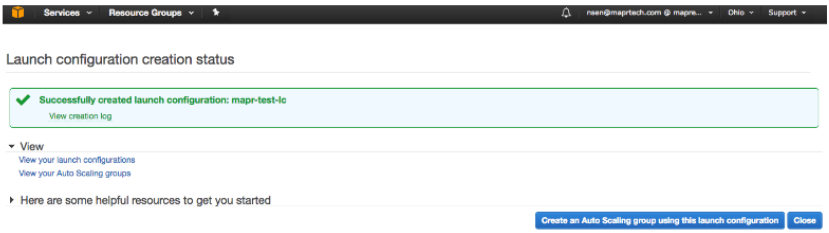

Services
Resource Groups
nsen@maprtech.com @ mapre...
Ohio
Support
1. Choose AMI
2. Choose Instance Type
3. Configure details
4. Add Storage
5. Configure Security Group
6. Review
Create Launch Configuration
Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.
Filter by:
All instance types
Current generation
Show/Hide Columns
Currently selected: m4.xlarge (13 ECUs, 4 vCPUs, 2.4 GHz, Intel Xeon E5-2676v3, 16 GiB memory, EBS only)
Family
Type
vCPUs
Memory (GiB)
Instance Storage (GB)
EBS-Optimized Available
Network Performance
General purpose
t2.nano
1
0.5
EBS only
-
Low to Moderate
General purpose
t2.micro
Free tier eligible
1
1
EBS only
-
Low to Moderate
General purpose
t2.small
1
2
EBS only
-
Low to Moderate
General purpose
t2.medium
2
4
EBS only
-
Low to Moderate
General purpose
t2.large
2
8
EBS only
-
Low to Moderate
General purpose
t2.xlarge
4
16
EBS only
-
Moderate
General purpose
t2.2xlarge
8
32
EBS only
-
Moderate
General purpose
m4.large
2
8
EBS only
Yes
Moderate
General purpose
m4.xlarge
4
16
EBS only
Yes
High
General purpose
m4.2xlarge
8
32
EBS only
Yes
High
General purpose
m4.4xlarge
16
64
EBS only
Yes
High
General purpose
m4.10xlarge
40
160
EBS only
Yes
10 Gigabit
General purpose
m4.16xlarge
64
256
EBS only
Yes
20 Gigabit
Compute optimized
c4.large
2
3.75
EBS only
Yes
Moderate
Compute optimized
c4.xlarge
4
7.5
EBS only
Yes
High
Compute optimized
c4.2xlarge
8
15
EBS only
Yes
High
Compute optimized
c4.4xlarge
16
30
EBS only
Yes
High
Cancel
Previous
Next: Configure details


Services
Resource Groups
nsen@maprtech.com @ mapre...
Ohio
Support
1. Choose AMI
2. Choose Instance Type
3. Configure details
4. Add Storage
5. Configure Security Group
6. Review
Copy Launch Configuration from mapr-test-lc
Name
mapr-test-lcCopy
Purchasing option
Request Spot instances
IAM role
None
Monitoring
Enable CloudWatch detailed monitoring
Learn more
EBS-optimized instance
Launch as EBS-optimized instance
Additional charges apply.
Advanced Details
Kernel ID
Use default
RAM Disk ID
Use default
User data
As text
As file
Input is already base64 encoded
(Optional)
IP Address Type
Only assign a public IP address to instances launched in the default VPC and subnet. (default)
Assign a public IP address to every instance.
Do not assign a public IP address to any instances.
Note: this option only affects instances launched into an Amazon VPC
Later, if you want to use a different launch configuration, you can create a new one and apply it to any Auto Scaling group. Existing launch configurations cannot be edited.
Cancel
Previous
Skip to review
Next: Add Storage


Services
Resource Groups
nsen@maprtech.com @ mapre...
Ohio
Support
1. Choose AMI
2. Choose Instance Type
3. Configure details
4. Add Storage
5. Configure Security Group
6. Review
Create Launch Configuration
Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes.
https://docs.aws.amazon.com/console/ec2/launchinstance/storage about storage options in Amazon EC2.
Volume Type
Device
Snapshot
Size (GiB)
Volume Type
IOPS
Throughput
Delete on Termination
Encrypted
Root
/dev/sda1
snap-0be6ed8d592a9b016
128
General Purpose (SSD)
384 / 3000
N/A
No
EBS
/dev/sdb
Search (case-insensitive)
20
General Purpose (SSD)
100 / 3000
N/A
EBS
/dev/sdc
Search (case-insensitive)
20
General Purpose (SSD)
100 / 3000
N/A
EBS
/dev/sdd
Search (case-insensitive)
20
General Purpose (SSD)
100 / 3000
N/A
Add New Volume
Free tier eligible customers can get up to 30 GB of EBS storage. Learn more about free usage tier eligibility and usage restrictions.
Cancel
Previous
Skip to review
Next: Configure Security Group


Services
Resource Groups
nsen@maprtech.com @ mapre...
Ohio
Support
1. Choose AMI
2. Choose Instance Type
3. Configure details
4. Add Storage
5. Configure Security Group
6. Review
Copy Launch Configuration from mapr-test-lc
A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.
Assign a security group:
Create a new security group
Select an existing security group
Security Group ID
Name
VPC ID
Description
Actions
sg-03ccf56a
anaik_nsg
vpc-44c4312d
anaik_nsg
Copy to new
sg-14fa927d
default
vpc-44c4312d
default VPC security group
sg-2ec13846
default
vpc-57a4ee3e
default VPC security group
sg-38311fd50
default
vpc-961845ff
default VPC security group
sg-3a3cca52
default
vpc-7e9cd317
default VPC security group
sg-7e18d716
default
vpc-c795c8ba
default VPC security group
sg-8228e5ea
default
vpc-9f2d7ff6
default VPC security group
sg-9a90a4f2
default
vpc-16f1a67f
default VPC security group
sg-9daf63f5
default
vpc-c669dba9
default VPC security group
sg-9e9657f6
default
vpc-b15908d8
default VPC security group
sg-9f5e91f7
default
vpc-8aacf1e3
default VPC security group
sg-e9814d81
default
vpc-5894c531
default VPC security group
sg-46323f2f
launch-wizard-1
vpc-44c4312d
launch-wizard-1 created 2017-06-27T10:57:30.880-03:00
sg-f4ab5b9c
launch-wizard-10
vpc-44c4312d
launch-wizard-10 created 2017-08-08T16:22:53.517-03:00
sg-c04ab2a9
launch-wizard-11
vpc-44c4312d
launch-wizard-11 created 2017-08-15T12:52:36.687-03:00
sg-20ea1948
launch-wizard-12
vpc-44c4312d
launch-wizard-12 created 2017-08-09T15:46:56.273-03:00
Inbound rules for sg-3ca16f54 Selected security groups: sg-9f5e91f7, sg-3ca16f54.
Type
Protocol
Port Range
Source
Custom TCP Rule
TCP
9443
0.0.0.0/0
Custom TCP Rule
TCP
8443
0.0.0.0/0
Cancel
Previous
Review


Services
Resource Groups
Ohio
Support
1. Choose AMI
2. Choose Instance Type
3. Configure details
4. Add Storage
5. Configure Security Group
6. Review
Create Launch Configuration
Review the details of your launch configuration. You can go back to edit the details of each section before you finish.
Your instance configuration is not eligible for the free usage tier
If you want to launch a free usage tier eligible instance, please check your AMI selection, instance type, configuration options, or storage devices. Learn more about free tier usage tier eligibility and usage restrictions.
Don't show me this again
AMI Details
Edit AMI
CentOS Linux 7 x86_64 HVM EBS 1703_01 - ami-9cbf9bf9
CentOS Linux 7 x86_64 HVM EBS 1703_01
Instance Type
Edit instance type
Instance Type
ECUs
vCPUs
Memory GiB
Instance Storage (GiB)
EBS-Optimized Available
Network Performance
m4.xlarge
13
4
16
EBS only
Yes
High
Launch configuration details
Edit details
Name
Purchasing option
On demand
EBS Optimized
No
Monitoring
No
IAM role
None
Tenancy
Shared tenancy (multi-tenant hardware)
Kernel ID
Use default
RAM Disk ID
Use default
User data
IP Address Type
Only assign a public IP address to instances launched in the default VPC and subnet. (default)
Storage
Edit storage
Security Groups
Edit security groups
Cancel
Previous
Create launch configuration
Select an existing key pair or create a new key pair
A key pair consists of a public key that AWS stores, and a private key file that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.
Choose an existing key pair
Select a key pair
key-awstestcluster2
I acknowledge that I have access to the selected private key file (key-awstestcluster2.pem), and that without this file, I won't be able to log into my instance.
Cancel
Create launch configuration

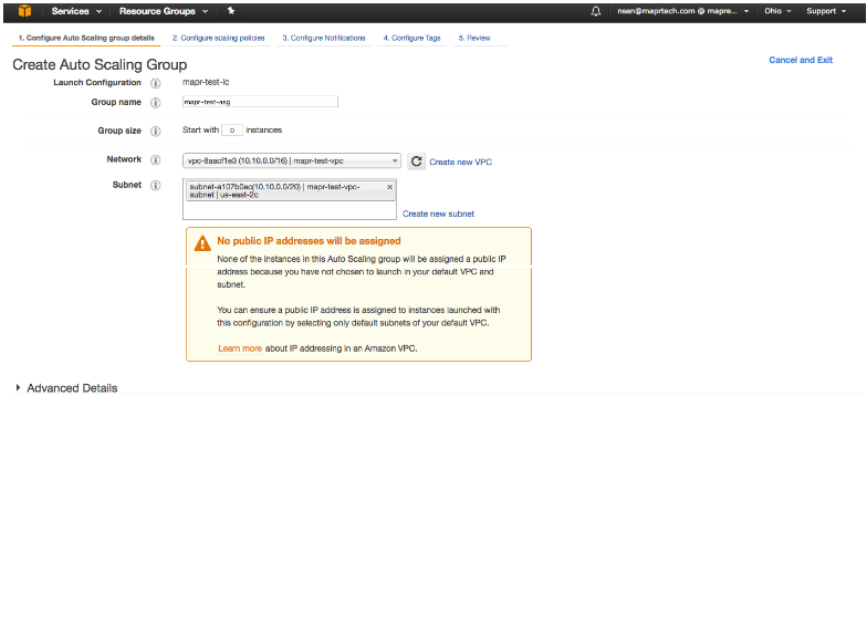


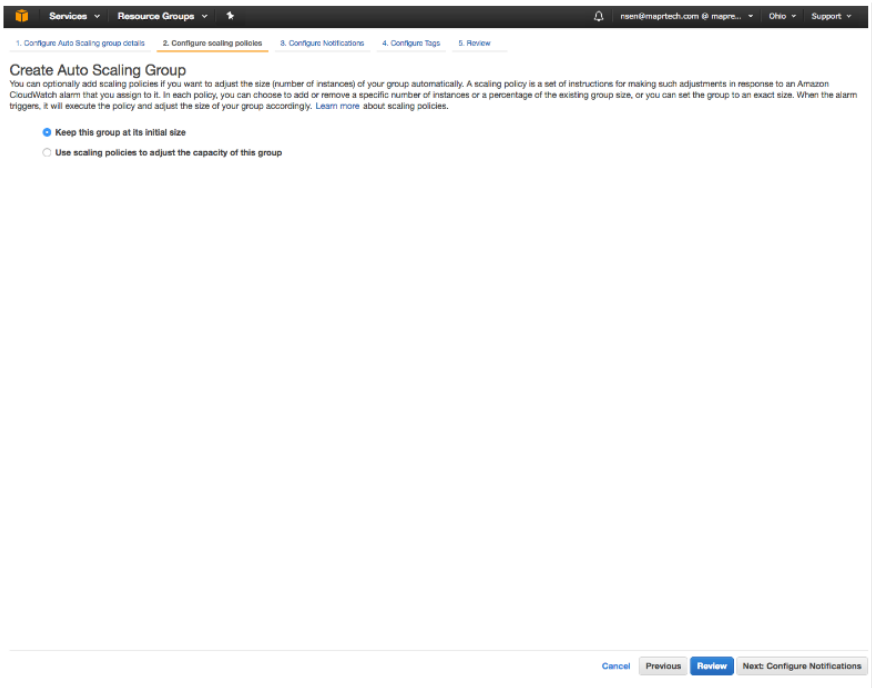
You can go on to creating an auto scaling group with the launch configuration created from the final screen.

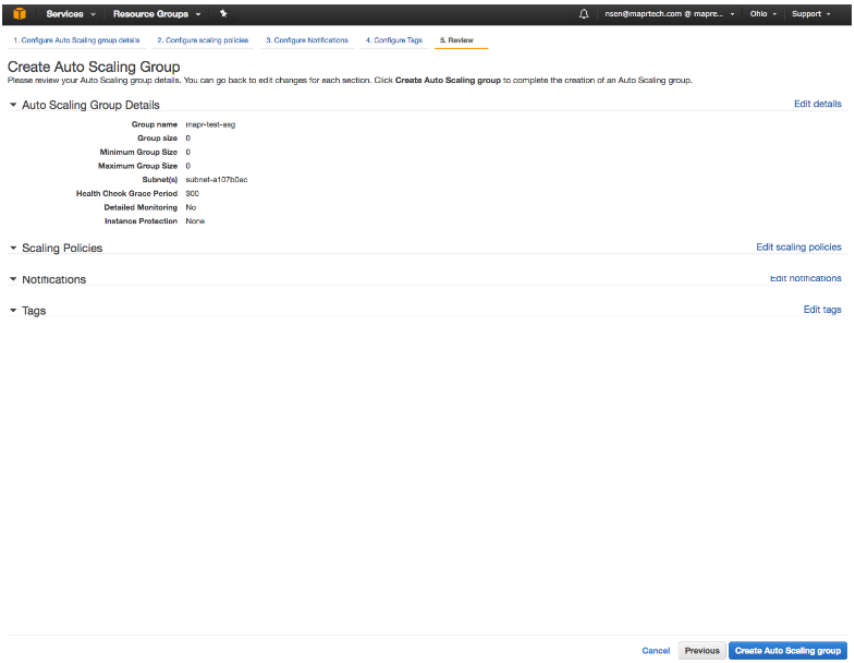
Create an Auto-scale Group

From AWS console, create auto scaling group:

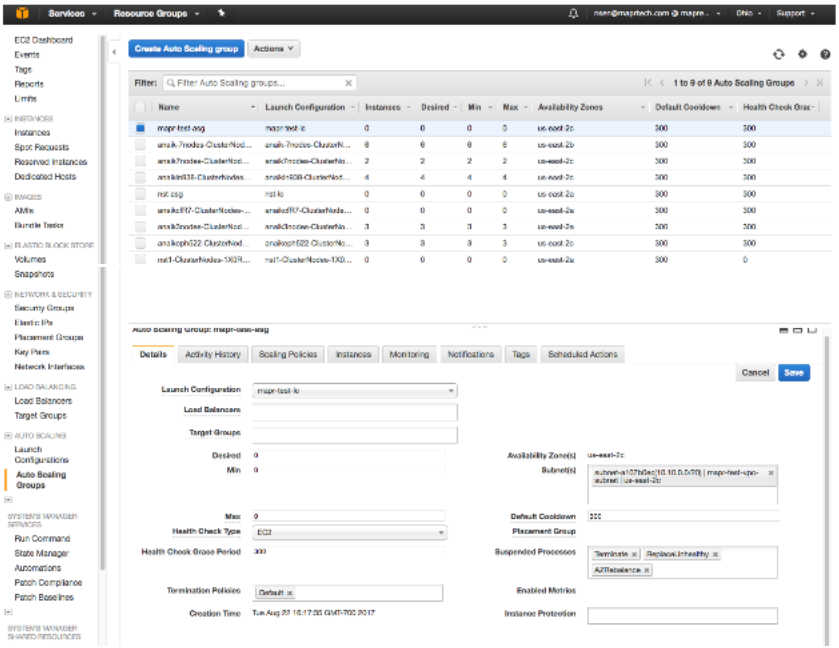
- Set auto-scale group properties
  - Give it a name
  - Select the VPC and the private-subnet
  - Choose 0 instances to start with (and let the MapR installer manage it)
- Select to keep the group at initial size
- After auto-scale group is created, edit the group to Suspend the following 4 services
  - Terminate, ReplaceUnhealthy, AZRebalance, HealthCheck


Services
Resource Groups
nsen@maprtech.com @ mapre...
Ohio
Support
1. Configure Auto Scaling group details
2. Configure scaling policies
3. Configure Notifications
4. Configure Tags
5. Review
Create Auto Scaling Group
Cancel and Exit
Launch Configuration
mapr-test-lc
Group name
mapr-test-asg
Group size
Start with 0 instances
Network
vpc-8aacf1e3 (10.10.0.0/16) | mapr-test-vpc
Create new VPC
Subnet
subnet-a107b0ec(10.10.0.0/20) | mapr-test-vpc-subnet | us-east-2c
Create new subnet
No public IP addresses will be assigned
None of the instances in this Auto Scaling group will be assigned a public IP address because you have not chosen to launch in your default VPC and subnet.
You can ensure a public IP address is assigned to instances launched with this configuration by selecting only default subnets of your default VPC.
Learn more about IP addressing in an Amazon VPC.
Advanced Details
Cancel
Next: Configure scaling policies


Services
Resource Groups
nsen@maprtech.com @ mapre...
Ohio
Support
1. Configure Auto Scaling group details
2. Configure scaling policies
3. Configure Notifications
4. Configure Tags
5. Review
Create Auto Scaling Group
You can optionally add scaling policies if you want to adjust the size (number of instances) of your group automatically. A scaling policy is a set of instructions for making such adjustments in response to an Amazon CloudWatch alarm that you assign to it. In each policy, you can choose to add or remove a specific number of instances or a percentage of the existing group size, or you can set the group to an exact size. When the alarm triggers, it will execute the policy and adjust the size of your group accordingly. Learn more about scaling policies.
Keep this group at its initial size
Use scaling policies to adjust the capacity of this group
Cancel
Previous
Review
Next: Configure Notifications



Suspend auto-scale management processes:



Create an EC2 instance for the installer

From AWS console, create an EC2 instance using an AMI with supported OS:

1. Assign it to the VPC created and public-subnet. Assign a public IP address.
2. Give role to be able to execute AWS commands without credentials
    1. Alternatively, create aws credentials files on the installer (see next section)
3. Min disk size: 128G
4. Assign the following security groups:
    1. Default security group to allow the node to talk to all nodes in the cluster
    2. The security group created to allow web access to the MapR services
    3. The security group created to allow SSH access to the nodes

Setup MapR installer

SSH to mapr installer and as root run:

Note: If the installer has not been setup with an IAM Role to allow it to execute AWS commands, follow the section "Create AWS credentials file" first.

Note: replace with the name of you wish to give your cluster

1. wget http://package.mapr.com/releases/installer/mapr-setup.sh (http://package.mapr.com/releases/installer/mapr-setup.sh)

2. chmod +x mapr-setup.sh
3. ./mapr-setup.sh -y
4. cd /opt/mapr/installer
5. source build/installer/bin/activate
6. cd data
7. ssh-keygen -b 2048 -t rsa -f -q -N '' -C "maprinstaller@maprcluster"
8. aws ec2 import-key-pair --key-name --region us-east-2 --public-key-material "`cat.pub`"
9. chmod 400
10. touch config.yml
11. chown mapr:mapr .pub config.yml
12. vi config.yml

Copy and paste the content below. Update the values as per your environment.

```
Environment:
     mapr_core_version: 5.2.2
    config:
     ssh_id: centos
     ssh_key_file: /opt/mapr/installer/data/<clustername>
     cluster_name: <clustername>
     mep_version: 3.0.1
     provider:
       id: AWS
       config:
         aws_region: us-east-2
         auto_scaling_group: mapr-test-asg
         count: 3
         key_name: <clustername>
         disk_type: gp2
         disk_size: 100
         disk_count: 3
     hosts: []
```

1. sudo -u mapr ../bin/mapr-installer-cli import -f -n --config -t config.yml
2. passwd mapr

Next, launch the installer and complete the rest of the installation via the installer. The installer would be listening on: https://:9443

Create AWS credentials file

If you did not create an AWS role to be used by the MapR installer, you must create an AWS credentials file with AWS access key and secret. Information on how to obtain access key and secret can be found at http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html (http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html)

1. mkdir -p ~/home/mapr/.aws

2. vi ~/home/mapr/.aws/credentials

```
[default]
    aws_access_key_id = <your aws access_key>
    aws_secret_access_key = <your aws secret key>
```

GET STARTED

Email Us (/company/contact-mapr/#contact-us)

+1 855-NOW-MAPR (tel:8556696277)

Download MapR for Free (/try-mapr/)

Request a Demo (/demo/)

Why MapR?
(/why-mapr/)

Customers (/customers/)

Solutions (/solutions/)

Products (/products/)

Company

(/company/)

Press (/company/press-releases/) | News (/company/news/)

Leadership (/company/leadership/)

Investors (/company/investors/)

Partners (/partners/)

Services (/services/)

Training (/training/)

Careers (/careers/)

Awards (/company/awards/)

Contact Us
(/company/contact-mapr/)

Contact Sales

(mailto:sales@mapr.com)

United States: +1 408-914-2390

(tel:4089142390)

Outside the US: +1 855-NOW-MAPR

(tel:8556696277)

Legal
(/legal/)

(https://www.linkedin.com/company/mapr-technologies)

(https://www.facebook.com/maprtech/) (https://twitter.com/mapr)

(https://www.youtube.com/user/maprtech) (/company/contact-mapr/)