

Read Now (/blog/dataware-the-most-important-software-abstraction-of-your-enterprise-it-stack/?source=12.19.18_REG-siteBanner)

Try MapR > AWS (</try-mapr/aws/>) > Manually Deploying

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:

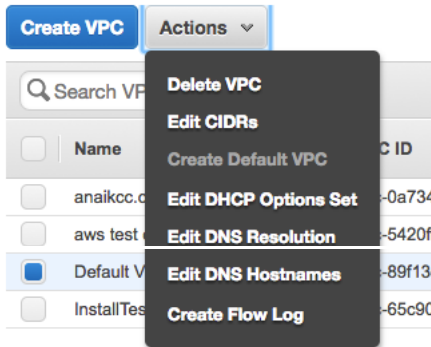
1. Create VPC
 1. Make sure that "DNS Resolution" and "DNS Hostnames" are enabled for the VPC
2. Create two subnets These will be configured such that one can be accessed from the Internet (public-subnet), another can talk to the Internet but cannot be accessed from outside (private-subnet)
3. Create 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
 2. Web Access
 1. Ports: 9443, 8443, 8042, 8047, 8088, 8888, 18080, 19888

Create VPC

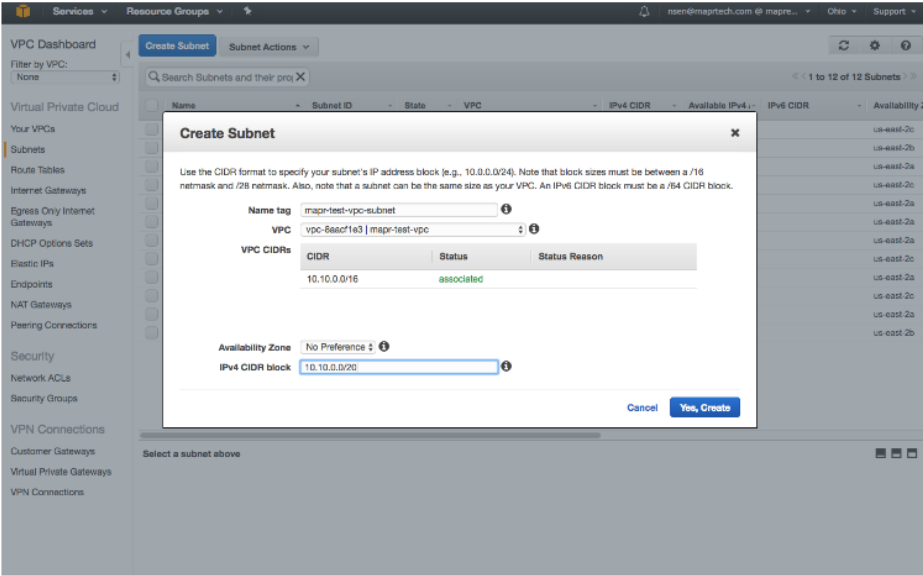
The screenshot shows the AWS Management Console interface. On the left is the 'VPC Dashboard' with a sidebar containing various VPC-related options like Subnets, Route Tables, and Internet Gateways. The main area displays the 'Create VPC' modal dialog. The dialog has a title bar with 'Create VPC' and a close button. Below the title is a descriptive text about VPCs. The form fields include: 'Name tag' with the value 'map-test-vpc', 'IPv4 CIDR block' with the value '10.10.0.0/16', 'IPv6 CIDR block' with radio buttons for 'No IPv6 CIDR Block' (selected) and 'Amazon provided IPv6 CIDR block', and 'Tenancy' set to 'Default'. At the bottom of the dialog are 'Cancel' and 'Yes, Create' buttons. In the background, a table of network ACLs is visible, showing columns for VPC ID, Subnet ID, Rule ID, Action, Protocol, Port Range, and Rule Name.

VPC ID	Subnet ID	Rule ID	Action	Protocol	Port Range	Rule Name
vpc-312bdc68	rtb-186da871	acl-cf788da6	Def			
vpc-312bdc68	rtb-c6362caf	acl-cc1bca87	Def			
vpc-312bdc68	rtb-919ab1b8	acl-b71c33d8	Def			
vpc-312bdc68	rtb-36wef51	acl-8e745705	Def			
vpc-312bdc68	rtb-168ba07f	acl-4b32056e	Def			
vpc-312bdc68	rtb-3f8ea456	acl-b65b06df	Def			
vpc-312bdc68	rtb-667c4b0f	acl-131b397a	Def			
vpc-312bdc68	rtb-478f712e	acl-dfb89b66	Def			
vpc-312bdc68	rtb-211fd448	acl-0503248c	Def			
vpc-312bdc68	rtb-8ab797f3	acl-4b5c38bdc	Def			

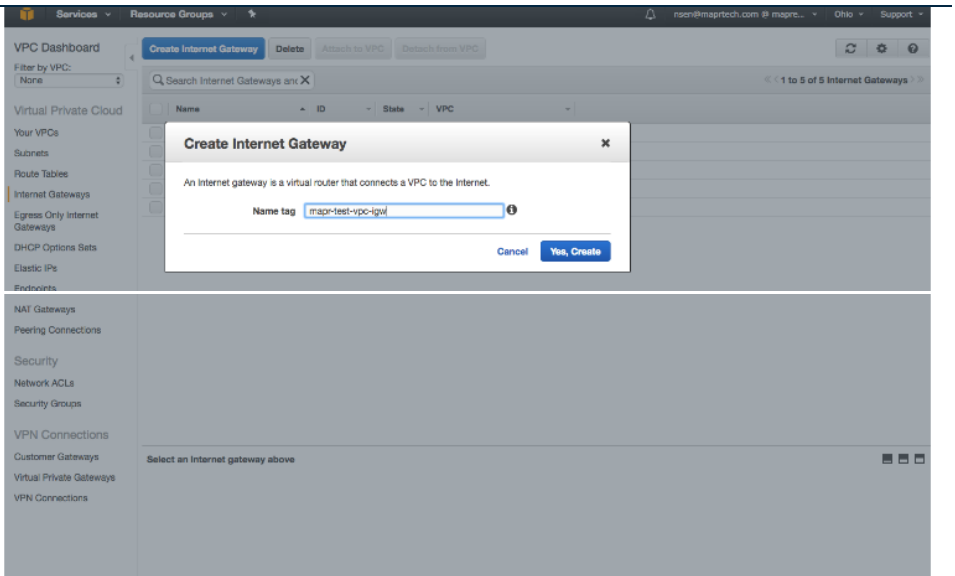
DNS Resolution and DNS Hostnames are enabled



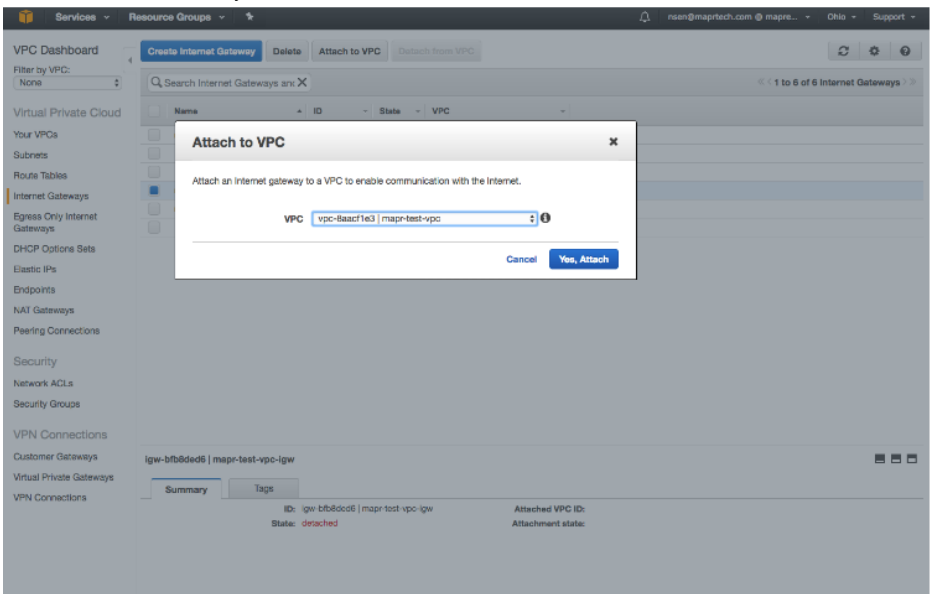
Create two subnets in the VPC you created above (you need to do this step twice - once for each subnet). The subnet CIDR should be different and non-overlapping for the two subnets. So, if your VPC CIDR is 10.10.0.0/16, your public subnet CIDR could be 10.10.0.0/24 and private subnet CIDR could be 10.10.8.0/22



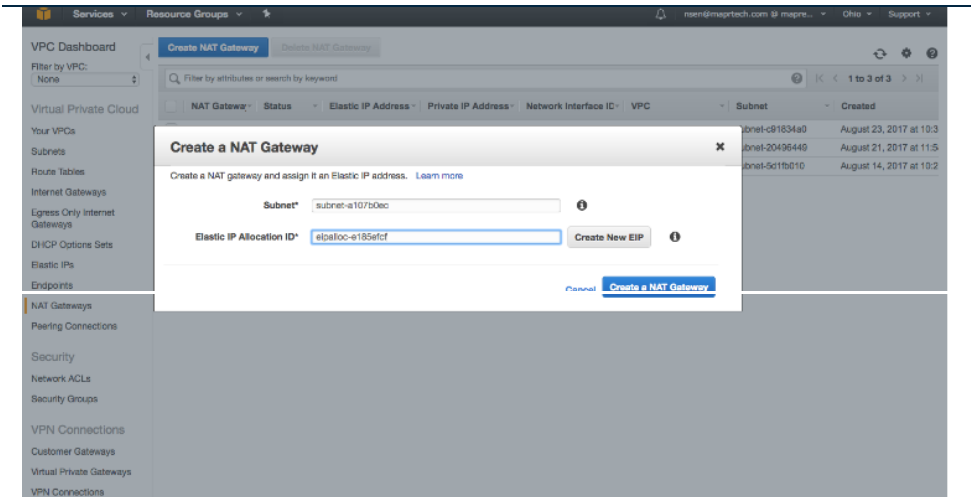
Create Internet Gateway



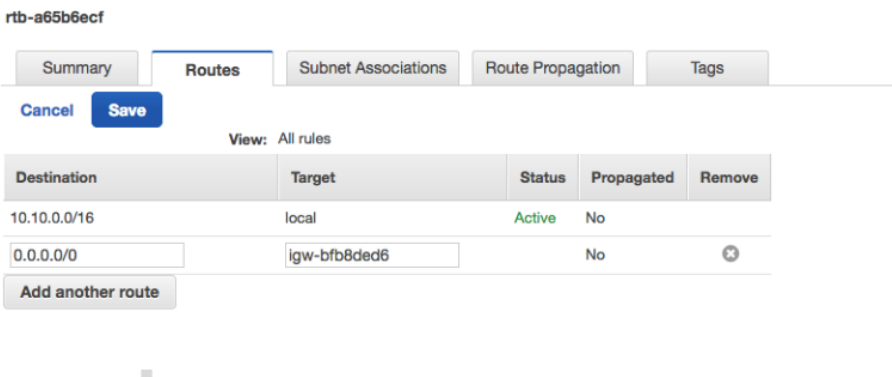
Attach Internet Gateway to VPC



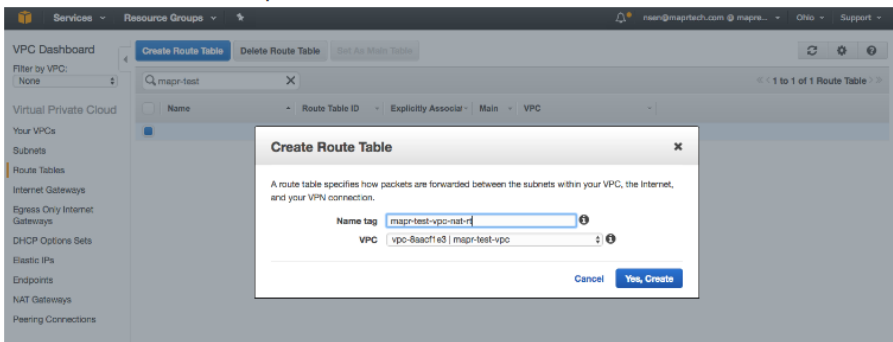
Create NAT Gateway - choose the public subnet



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



Create a new route table for private subnet



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

rtb-1b734772 | mapr-test-vpc-nat-rt

Summary Routes Subnet Associations Route Propagation Tags

Edit

View: All rules

Destination	Target	Status	Propagated
10.10.0.0/16	local	Active	No
0.0.0.0/0	nat-08b93cb8fa7fe50e2	Active	No

Associate route table with the private subnet

Associate route table with the private subnet

rtb-1b734772 | mapr-test-vpc-nat-rt

Summary Routes Subnet Associations Route Propagation Tags

Cancel Save

Associate	Subnet	IPv4 CIDR	IPv6 CIDR	Current Route Table
<input type="checkbox"/>	subnet-a107b0ec mapr-test-vpc-subnet	10.10.0.0/20	-	Main
<input checked="" type="checkbox"/>	subnet-4379cf0e mapr-test-vpc-subnet	10.10.255.0/24	-	Main

rtb-1b734772 | mapr-test-vpc-nat-rt

Summary Routes Subnet Associations Route Propagation Tags

Edit

Subnet	IPv4 CIDR	IPv6 CIDR
subnet-4379cf0e mapr-test-vpc-subnet	10.10.255.0/24	-

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Subnet	IPv4 CIDR	IPv6 CIDR
subnet-a107b0ec mapr-test-vpc-subnet	10.10.0.0/20	-

Create Security Groups

Services Resource Groups

VPC Dashboard

Create Security Group Security Group Actions

Filter by VPC: None

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHOP Options Sets

Elastic IPs

Endpoints

NAT Gateways

Peering Connections

Security

Network ACLs

Security Groups

VPN Connections

Customer Gateways

Virtual Private Gateways

VPN Connections

Filter All security groups Search Security Groups and t

Create Security Group

Name tag mapr-test-webaccess

Group name mapr-test-webaccess

Description mapr-test-webaccess

VPC vpc-baacf1e3 | mapr-test-vpc

Cancel Yes, Create

Add Inbound security rules

sg-3ca16f54 | mapr-test-webaccess

Summary

Inbound Rules

Outbound Rules

Tags

Edit

Type	Protocol	Port Range	Source
Custom TCP Rule	TCP (6)	9443	0.0.0.0/0
HTTPS* (8443)	TCP (6)	8443	0.0.0.0/0

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

The screenshot displays the AWS Management Console interface for creating a launch configuration. The top navigation bar shows the user is logged in as 'nser@mapstech.com @ mapre...'. The main heading is 'Create Launch Configuration'. Below the heading, there are six steps: 1. Choose AMI, 2. Choose Instance Type, 3. Configure details, 4. Add Storage, 5. Configure Security Group, and 6. Review. The 'Choose AMI' step is currently active. On the left, there is a sidebar with 'Quick Start' and 'My AMIs' sections. The 'Community AMIs' section is expanded, showing a list of operating systems and architectures. The 'Operating system' section is checked, and the 'Architecture' section is set to 'x86_64'. The 'Root device type' is set to 'EBS'. In the main area, a search bar contains the text 'ami-9cbr9t9f'. Below the search bar, the 'CentOS Linux 7 x86_64 HVM EBS 1703_01 - ami-9cbr9t9f' AMI is displayed. The 'Root device type' is 'EBS' and the 'Virtualization type' is 'HVM'. A 'Select' button is visible next to the AMI.

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 typesCurrent generationShow/Hide Columns

Currently selected: m4.xlarge (13 ECUs, 4 vCPUs, 2.4 GHz, Intel Xeon E5-2670v3, 16 GiB memory, EBS only)							
	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance
	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate
	General purpose	t2.micro	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

CancelPreviousNext: Configure details

ServicesResource Groups

nsr@maptech.com @ mapre...OnbSupport

1. Choose AMI2. Choose Instance Type3. Configure details4. Add Storage5. Configure Security Group6. Review

Copy Launch Configuration from mapr-test-ic

Name

mapr-test-icCopy

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 textAs fileInput 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.

CancelPreviousSkip to reviewNext: Add Storage

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> for additional storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput	Delete on Termination	Encrypted
Root	/dev/xda1	snap-0be6ed8d1f02a0b016	128	General Purpose (SSD)	384 / 3000	N/A	<input checked="" type="checkbox"/>	No
EBS	/dev/sdb	<input type="text" value="Search (case-insensitive)"/>	20	General Purpose (SSD)	100 / 3000	N/A	<input checked="" type="checkbox"/>	<input type="checkbox"/>
EBS	/dev/sdc	<input type="text" value="Search (case-insensitive)"/>	20	General Purpose (SSD)	100 / 3000	N/A	<input checked="" type="checkbox"/>	<input type="checkbox"/>
EBS	/dev/sdd	<input type="text" value="Search (case-insensitive)"/>	20	General Purpose (SSD)	100 / 3000	N/A	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Add New Volume

Free tier eligible customers can get up to 30 GiB of EBS storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Copy Launch Configuration from mapr-test-ic

A security group is a set of firewall rules that control the traffic for your instances. 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
<input type="checkbox"/> sg-03ccf56a	anaik_nsg	vpc-44a4312d	anaik_nsg	Copy to new
<input type="checkbox"/> sg-14f6d27d	default	vpc-44a4312d	default VPC security group	Copy to new
<input type="checkbox"/> sg-2ec1384d	default	vpc-674ae3e	default VPC security group	Copy to new
<input type="checkbox"/> sg-3031f050	default	vpc-66194bf	default VPC security group	Copy to new
<input type="checkbox"/> sg-3a30ca52	default	vpc-769cd317	default VPC security group	Copy to new
<input type="checkbox"/> sg-7e18d716	default	vpc-2795c08a	default VPC security group	Copy to new
<input type="checkbox"/> sg-4228f5ea	default	vpc-692d7f85	default VPC security group	Copy to new
<input type="checkbox"/> sg-9e90a4f2	default	vpc-1618a67f	default VPC security group	Copy to new
<input type="checkbox"/> sg-9da5f3f5	default	vpc-c089dba9	default VPC security group	Copy to new
<input type="checkbox"/> sg-9e065786	default	vpc-b15908d8	default VPC security group	Copy to new
<input checked="" type="checkbox"/> sg-9f5e91f7	default	vpc-6aac1e3	default VPC security group	Copy to new
<input type="checkbox"/> sg-e9814d81	default	vpc-6894cd31	default VPC security group	Copy to new
<input type="checkbox"/> sg-463232d7	launch-wizard-1	vpc-44a4312d	launch-wizard-1 created 2017-06-27T10:57:30.880-03:00	Copy to new
<input type="checkbox"/> sg-44a0b0fc	launch-wizard-10	vpc-44a4312d	launch-wizard-10 created 2017-08-08T16:22:53.517-03:00	Copy to new
<input type="checkbox"/> sg-c04abca0	launch-wizard-11	vpc-44a4312d	launch-wizard-11 created 2017-08-15T12:52:36.687-03:00	Copy to new
<input type="checkbox"/> sg-20ea1948	launch-wizard-12	vpc-44a4312d	launch-wizard-12 created 2017-08-09T15:46:58.273-03:00	Copy to new

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	9443	0.0.0.0/0

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-9cbf9b9f

CentOS Linux 7 x86_64 HVM EBS 1703_01

Root device type: xfs Virtualization type: hvm

Instance Type

[Edit instance type](#)

Instance Type	ECUs	vCPUs	memory GiB	Instance storage (GiB) IOPS	FAFS-Optimized Available	Network Performance
m4.xlarge	13	4	16	EBS only	Yes	High

Launch configuration details

[Edit details](#)

Name	mapre-test-1c
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**

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-9cbf9b9f

CentOS Linux 7 x86_64 HVM EBS 1703_01

Root device type: xfs Virtualization type: hvm

Instance Type

[Edit instance type](#)

Instance Type	Instance Storage (GiB) IOPS	EBS-Optimized Available	Network Performance
m4.xlarge	EBS only	Yes	High

Launch configuration details

[Edit details](#)

Name	mapre-test-1c
Purchasing option	On demand
EBS Optimized	No
Monitoring	No
IAM role	None
Tenancy	Shared
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)

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-avstestcluster2

☒ I acknowledge that I have access to the selected private key file (key-avstestcluster2.pem), and that without this file, I won't be able to log into my instance.

Cancel

Create launch configuration

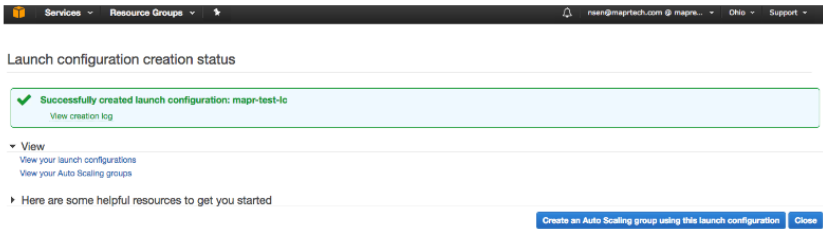
Storage

[Edit storage](#)

Security Groups

[Edit security groups](#)

Cancel Previous **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

ServicesResource Groups

nen@maptech.com @ mapre...OhioSupport

1. Configure Auto Scaling group details2. Configure scaling policies3. Configure Notifications4. Configure Tags5. Review

Create Auto Scaling Group

Launch Configuration

Group name

Group size

Network

Subnet

Create new VPC

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

ServicesResource Groups

nen@maptech.com @ mapre...OhioSupport

1. Configure Auto Scaling group details2. Configure scaling policies3. Configure Notifications4. Configure Tags5. 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

CancelPreviousReviewNext: Configure Notifications

ServicesResource Groups

nsen@maptech.com @ mapre...OhioSupport

1. Configure Auto Scaling group details2. Configure scaling policies3. Configure Notifications4. Configure Tags5. Review

Create Auto Scaling Group

Please review your Auto Scaling group details. You can go back to edit changes for each section. Click **Create Auto Scaling group** to complete the creation of an Auto Scaling group.

▼ Auto Scaling Group Details

Group name

mapr-test-sig

Group size

0

Minimum Group Size

0

Maximum Group Size

0

Subnet(s)

subnet-a107b0ae

Health Check Grace Period

300

Detailed Monitoring

No

Instance Protection

None

Edit details

▼ Scaling Policies

Edit scaling policies

▼ Notifications

Edit notifications

▼ Tags

Edit tags

CancelPreviousCreate Auto Scaling group

Suspend auto-scale management processes:

The screenshot displays the AWS Management Console interface for creating an Auto Scaling group. The left sidebar shows the navigation menu with categories like INSTANCES, RANGES, ELASTIC BLOCK STORE, NETWORK & SECURITY, and SYSTEMS MANAGER. The main content area shows the 'Create Auto Scaling group' wizard. The 'Launch Configuration' step is active, showing a table of existing launch configurations. Below the table, the 'Launch Configuration' dropdown is set to 'mapr-test-ec2'. The 'Launch Configuration' section shows 'Launch Configuration' as 'mapr-test-ec2', 'Load Balancers' as empty, and 'Target Groups' as empty. The 'Desired' and 'Min' values are 0, and the 'Max' value is 0. The 'Health Check Type' is 'EC2' and the 'Health Check Grace Period' is '300'. The 'Termination Policies' are set to 'Default'. The 'Availability Zones' section shows 'us-east-2c' as the selected zone. The 'Default Cooldown' is '300'. The 'Suspended Processes' section shows 'Terminate' and 'Rebalance' as selected. The 'Enabled Metrics' section shows 'AllInstance' as selected. The 'Instance Protection' section is empty.

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/)

[Careers \(/careers/\)](/careers/)

Training (/training/)

[Awards \(/company/awards/\)](/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/)

