Containers

Upcoming Changes to IP Assignment for EKS Managed Node Groups

by Nathan Taber | on 26 MAR 2020 | in Amazon Elastic Kubernetes Service, Announcements, Containers, Top Posts | Permalink | Comments | Share

When using Amazon EKS, all nodes need the ability to connect to the EKS-hosted Kubernetes cluster and to other AWS APIs such as Amazon Elastic Container Registry (ECR) or Amazon S3. Nodes can run in private or public subnets. For private subnets, this traffic typically routes through an AWS PrivateLink connection to reach endpoints within the VPC or a NAT gateway to reach endpoints outside of the VPC. For public subnets, your nodes need a public IP assigned in order to reach API endpoints outside of the VPC.

Today, an EKS managed node group automatically assigns public IP addresses to **all nodes** that it launches. When a public IP address is assigned using the `AssociatePublicIpAddress` flag on an EC2 instance or launch template, it overrides the settings in the subnet. This means that if your VPC is configured with the public + private subnet or private only subnet architectures, public IPs are still assigned to the nodes that are instantiated in the private subnets.

Starting ~~April 20, 2020~~ **April 22,2020**, we'll be updating the behavior of managed nodes groups to **no longer assign public IPs to nodes**. After this date, public IP assignment must be controlled via the subnet settings where the node is instantiated.

This change will only affect new managed node groups **created on or after** ~~April 20th~~ **April 22nd**, the behavior of existing managed node groups *will not change*.

Check your public subnet settings!

If you are using managed node groups with a public subnet, this change could mean that new nodes from new node groups may be **unable to connect to the cluster** if `mapPublicIpOnLaunch` is not set to **TRUE** for the public subnet. Before April 22, be sure to check your subnet settings and update the `mapPublicIpOnLaunch` to **TRUE** to ensure you do not have any issues.

To check the subnet settings for your VPC, run:

```
$ aws ec2 describe-subnets \
--filters "Name=vpc-id,Values=<VPC-ID>" | grep
'MapPublicIpOnLaunch\|SubnetId\|VpcId\|State'
```

Output:

```
$ aws ec2 describe-subnets     \
  --filters "Name=vpc-id,Values=vpc-0a78a1eac2c6f1c97" | grep 'MapPublicIpOnLaunch\|Sul

            "MapPublicIpOnLaunch": false,
```

```
            "State": "available",
            "SubnetId": "subnet-077ef53ee69f8a96c",
            "VpcId": "vpc-0a78a1eac2c6f1c97",

            "MapPublicIpOnLaunch": false,
            "State": "available",
            "SubnetId": "subnet-00bbcb7727a6e480a",
            "VpcId": "vpc-0a78a1eac2c6f1c97",

            "MapPublicIpOnLaunch": false,
            "State": "available",
            "SubnetId": "subnet-0b53021b40ff722f3",
            "VpcId": "vpc-0a78a1eac2c6f1c97",

            "MapPublicIpOnLaunch": false,
            "State": "available",
            "SubnetId": "subnet-0c1c2cc106c3fa4e2",
            "VpcId": "vpc-0a78a1eac2c6f1c97",

            "MapPublicIpOnLaunch": false,
            "State": "available",
            "SubnetId": "subnet-067f724fbaf58996c",
            "VpcId": "vpc-0a78a1eac2c6f1c97",

            "MapPublicIpOnLaunch": false,
            "State": "available",
            "SubnetId": "subnet-041c3fe623abcb488",
            "VpcId": "vpc-0a78a1eac2c6f1c97",
```


To update your subnet settings, you can manually change the `mapPublicIpOnLaunch` flag to **TRUE** using the AWS console, or by updating the CFN template.

Changes to the EKS node and VPC CloudFormation templates

To help make this switch easier, we're updating the EKS VPC and node CloudFormation templates. Previously, Amazon EKS vended AWS CloudFormation templates that assigned public IP addresses to worker nodes via the **EC2 configuration** instead of at the subnet.

Starting today, we are launching updated AWS CloudFormation templates that set the public IP assignment at the **subnet** for public subnets and are **removing the public IP assignment from node group templates.**

The new AWS CloudFormation VPC and self-managed worker node templates do not set the `AssociatePublicIpAddress` flag, and public subnets set the `mapPublicIpOnLaunch` flag to **TRUE**.

We're also updating eksctl in the coming weeks to match these changes. Our goal is that all clusters going forward assign public IPs via the subnet (when appropriate), instead of through the EC2 configuration.

The new VPC templates can be found in the EKS documentation.

Conclusion

If you are using Managed Node Groups and public subnets, be sure that you update your subnet settings to map public IPs on launch before ~~April 20~~ **April 22**. You can follow the progress of the updates to managed node groups on our GitHub roadmap.

If you want to learn more about networking configurations and IP assignment for EKS clusters, check out our blog on cluster networking for worker nodes.

— Nate
TAGS: EKS, managed nodes, networking

Comments

7 Comments

4 Prashanth ▾

Join the discussion...

♡ Share

Best Newest Oldest

Nathan Taber

4 years ago

@Tomáš Hrabec @RubenD This change was released 4/22 at 1PM PST - so if you created node groups after this time, they should have the new behavior.

@Kate Marshall saw your comments on GitHub. Check out the 'Private Only Subnets' section of our cluster networking blog: https://aws.amazon.com/blog...

You will need to turn on private link for EC2 and ECR in order to ensure that the nodes can download the container images required for them to connect to the control plane when they boot.

o o Reply

Kate Marshall

4 years ago

Hi Nathan! Is there a way to choose to associate public IP addresses on node groups via CFT, for example? I am working in a private subnets so its not advisable for me to make the changes suggested on this article, but my nodes are no longer able to connect to the control plane now that there is no public IPs associated. Any help would be greatly appreciated :-)

o o Reply

Chris

4 years ago

Any updates on this ?

o o Reply

saggi

4 years ago

when do we plan to release the fix ?

o o Reply

Nathan Taber ↗ saggi

4 years ago edited

This change will be released on April 22, 2020

1 0 Reply

T **Tomáš Hrabec** Nathan Taber

4 years ago

Hi Nathan, is there any exact time today when this will be released? The thing is I 5 minutes ago created new node group in private subnet and the EC2 instance got the public IP.

Thank you, Tomas.

0 0 Reply

R **RubenD** Nathan Taber

4 years ago

Is there more precise timeframe for this ?

0 0 Reply