



Customizing Managed Nodes in Amazon EKS

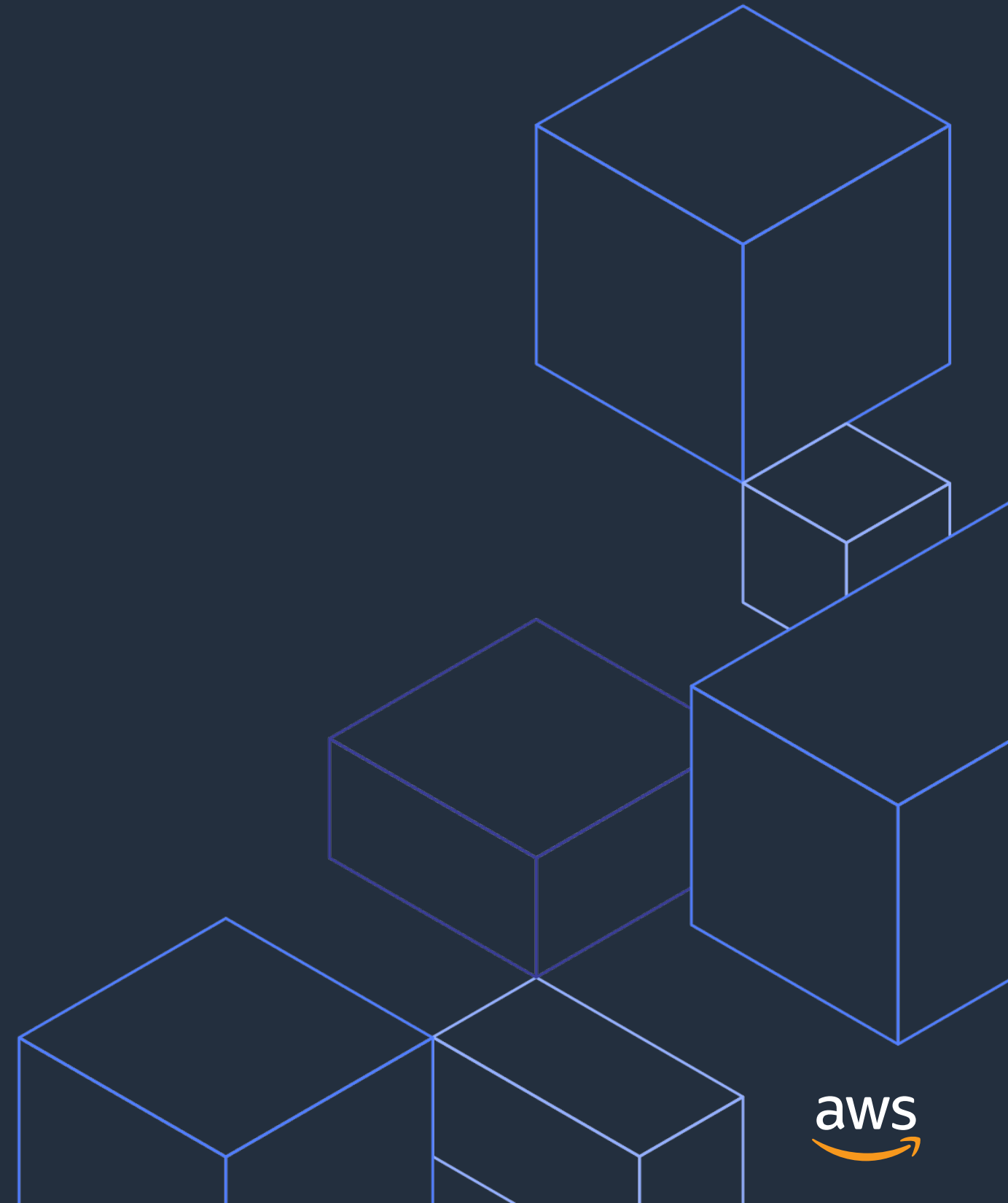
Launch Templates and Custom AMIs for Managed Node Groups

Jesse Butler, Sr. Developer Advocate
AWS Container Services

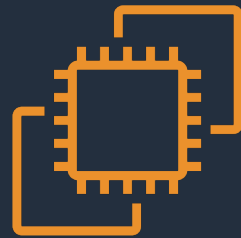
Agenda

- Amazon EKS Managed Node Groups
- Launch Templates for Managed Node Groups
- Custom AMIs for Managed Node Groups

Amazon EKS Managed Node Groups

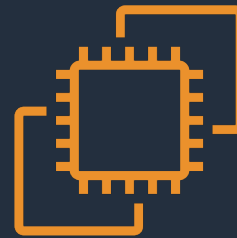


EKS Data Plane



Bring Your Own EC2 Nodes

Bring your own Autoscaling Groups running your own custom AMI. You are responsible for patching and the underlying OS.



Managed Node Groups

Provisioned by EKS in your VPC. They run the latest EKS optimized AMI. Handles automatic draining and rolling out new AMIs.



AWS Fargate

Containers running with no infrastructure in your account. They are right sized for your workload. Patching is fully managed.

Some Restrictions May Apply

Managed Node Groups use opinionated configuration for best out-of-the-box outcomes

Nodes are provisioned with an Amazon Linux-based AMI optimized for EKS use

Not well-aligned with some needs

- Additional software installation and configuration
- Enhanced security and compliance requirements
- Custom AMIs

Introducing Managed Node Customization

Launch Templates

- Declarative instance configuration and customization for managed nodes

Custom AMIs

- For deeper customization needs, or when a custom AMI is required

Launch Templates for Managed Node Groups



Managed Node Group Use Cases

Declarative configuration for EKS nodes

- Instance type, tags, disk configuration, etc

Light customization of node configuration

- Runtime configuration changes
- Additional software installation

```
{
  "LaunchTemplateData": {
    "EbsOptimized": false,
    "InstanceType": "t3.small",
    "KeyName": "bastion",
    "UserData": "TU\u001bNRS1WZXJzaW9uOiAxLjAKQ2
9udGVudC1UeXBloibtdWx0aXBhcnQvbWl4ZWQ7IGJvdW5kY
XJ5PSIvLyIKCi0tLy8KQ29udGVudC1UeXBloib0ZXh0L3gt
c2h1bGxzY3JpcHQ7IGNoYXJzZXQ9InVzLWFzY2lpIgojIS9
iaW4vYmFzaAoKeXVtIGluc3RhbGwgLXkgYW1hem9uLXNzbS
1hZ2VudApzeXN0ZW1jdGwgZW5hYmxlIGFtYXpvbi1zc20tY
WdlbnQgJiYgc3lzdGVtY3RsIHN0YXJ0IGFtYXpvbi1zc20t
YWdlbnQKLS0vLy0tCg==",
    "SecurityGroupIds": [
      "sg-0e9b58499f42bcd4b",
      "sg-0275026e71e1e7c9c"
    ]
  }
}
```


Using Launch Templates with Managed Node Groups

Create a Launch Template

Specify the template when creating a Managed Node Group
(API, CLI, Console, eksctl)

Update also supports Launch Templates, cycling the nodes
gracefully to the new configuration

Using Launch Templates with Managed Node Groups

Specified in the Launch Template configuration

- Instance type
- Disk size
- Remote access configuration
 - EC2 ssh key
 - Security groups

Specified in the Node Group API configuration

- Instance role
- Network subnets

Updating Managed Node Groups

Managed Node Groups can be updated with a new version of a Launch Template

Nodes are cycled gracefully, landing at the new specified configuration

Note, existing node groups cannot be migrated to using a Launch Template

Support for Launch Templates in eksctl

Specify a Launch Template version for cluster and node group operations

If no Launch Template is specified, one is created automatically and used

```
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
  name: luna
  region: us-west-2
  version: '1.17'

managedNodeGroups:
- name: luna-mng-custom-lt
  desiredCapacity: 2
  labels: {role: worker}
  launchTemplate:
    id: lt-00be677d795136d27
    version: 1
```

Launch Template User Data

Launch Templates may contain User Data specification

Instance configuration via shell scripts or cloud-init directives

- Add users and groups
- Install software packages
- Modify configuration
- Enable or disable services

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="//"

--//
Content-Type: text/x-shellscript; charset="us-ascii"
#!/bin/bash

yum install -y amazon-ssm-agent
systemctl enable amazon-ssm-agent && \
    systemctl start amazon-ssm-agent
--//--
```

Custom AMIs for Managed Node Groups



Custom AMIs for Managed Node Groups

EKS Managed Nodes are by default provisioned with EKS-optimized AMIs

Custom AMIs for any number of reasons

- Security or hardening compliance
- Org-standard distros

Any AMI that can serve as an EKS node is supported

Note, existing Managed Node Groups cannot migrate to Custom AMIs

Using Custom AMIs with Managed Node Groups

Specified in Launch Template configuration

- Image ID
- User Data

Note, when using a Custom AMI, some fields cannot be set in the API

- AMI Type
- Release version, version

Custom AMI Resources

- <https://github.com/awslabs/amazon-eks-ami>
- <https://github.com/aws-samples/amazon-eks-custom-amis>

Using Custom AMIs with Managed Node Groups

Note, when using a Custom AMI, user data is not merged with EKS node bootstrap

You must specify this as part of your User Data scripts

For nodes on private networks, ensure you include the EKS endpoint and API cert

Custom AMIs and eksctl

Launch Templates with Custom AMIs can be specified by ID and version

When no Launch Template is specified

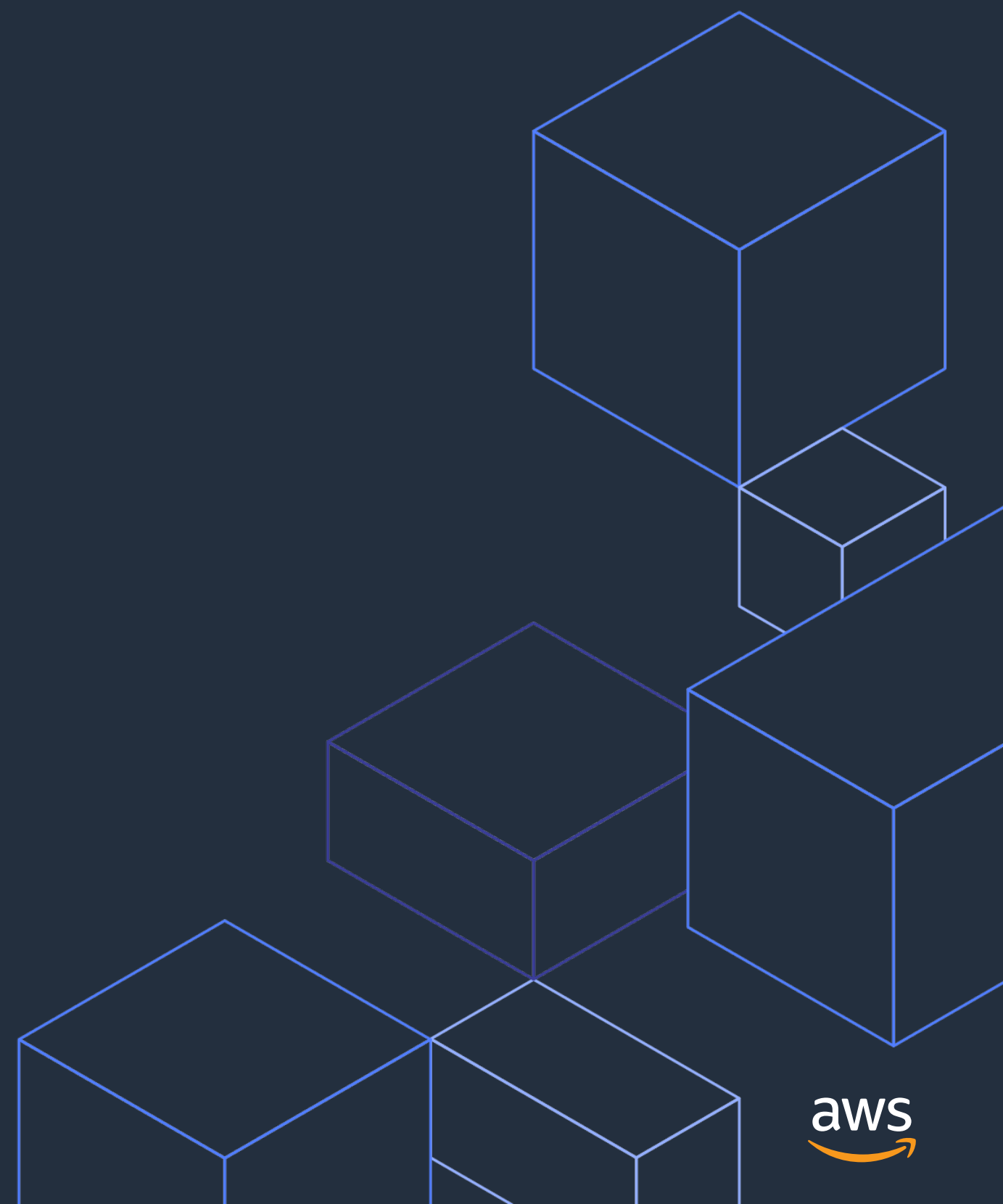
- Set the ami configuration element
- Use `overrideBootstrapCommand`

```
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
  name: ginny
  region: us-west-2
  version: '1.17'

managedNodeGroups:
- name: ginny-mng-custom-ami
  instanceType: t3.small
  desiredCapacity: 2
  labels: {role: worker}
  ami: ami-0030109261aa0205b
  ssh:
    publicKeyName: bastion
  preBootstrapCommands:
  - kubelet --version > /etc/eks/test-preBootstrapCom
mands
  overrideBootstrapCommand: |
    #!/bin/bash
    set -ex
    /etc/eks/bootstrap.sh ginny --kubelet-extra-args
'--node-labels=alpha.eksctl.io/cluster-name=ginny,alp
ha.eksctl.io/nodegroup-name=ginny-mng-custom-ami,eks.
amazonaws.com/nodegroup=ginny-mng-custom-ami,eks.amaz
onaws.com/nodegroup-image=ami-0030109261aa0205b'
```

Summary



Customizing Managed Node Groups in EKS

EKS Managed Node Groups provide provisioning and lifecycle management automation for your EKS nodes

Managed Node Groups can now be customized with support for EC2 Launch Templates, providing declarative configuration for nodes

Custom AMIs can now be used to create Managed Node Groups, and can be updated to new versions of, or even to different Custom AMIs



butlerjl@amazon.com

@jlb13

<https://github.com/aws/containers-roadmap>

