AWS re:Invent

NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

CON201

Best practices for using Amazon EKS add-ons

Jeremy Cowan

Principal Developer Advocate,
AWS Container Services
AWS

Sriram Ranganathan (He/Him)

Sr. Product Manager,
Amazon EKS
AWS

Agenda

Extending lifecycle management with Amazon EKS add-ons

Recent improvements

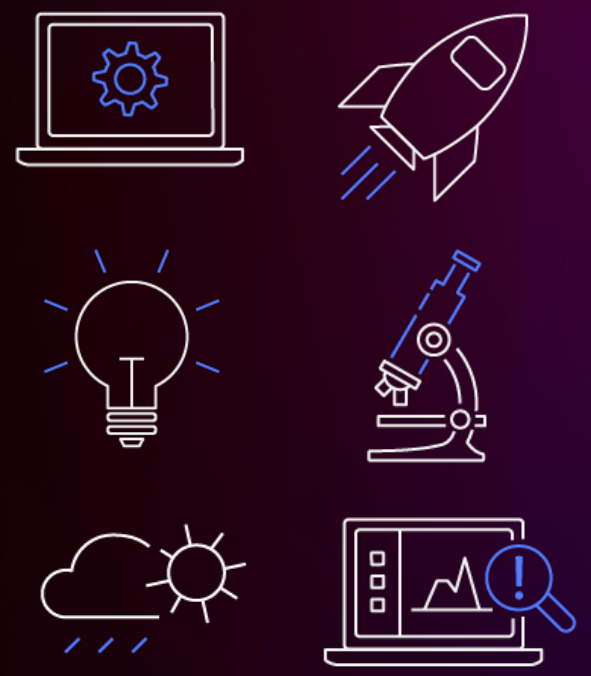
AWS Marketplace integration for Amazon EKS add-ons

Best practices

Amazon EKS is Kubernetes

Amazon EKS

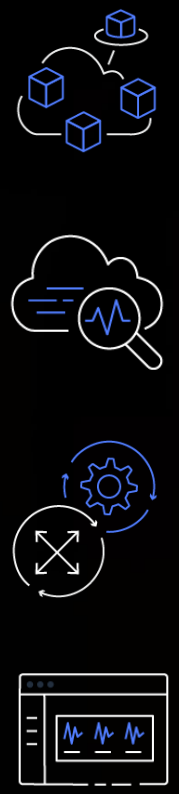
- A native Kubernetes experience delivered as a service by AWS
- Users leverage an amazing system of open-source solutions
- Amazon EKS provides native, well-integrated solutions into the AWS Cloud



We consider user experience to be our top feature, understanding that simplicity is powerful

AWS container services priorities

Amazon EKS add-ons



- Curated list of operational cluster software
- Built and tested together to work with Amazon EKS
- Enable during cluster creation or any time
- Single operation enable, disable, and update
- Uses worker node IAM role by default
- IAM role for service accounts for finer granularity
- Requires minimum Kubernetes v1.18 and eks.3

Amazon EKS add-ons in console

EKS > Clusters > addons-demo

addons-demo

Delete cluster

Cluster info Info

Kubernetes version Info	Status	Provider
1.24	Active	EKS

Overview | Resources | Compute | Networking | Add-ons | Authentication | Logging | Update history | Tags

Add-ons (3) Info

View details | Edit | Remove | Get more add-ons

Find add-on | Any category | Any status

1

CoreDNS
Enable service discovery within your cluster.

Category	Status	Version	IAM Role
networking	Active	v1.8.7-eksbuild.3	Inherited from node

kube-proxy
Enable service networking within your cluster.

Category	Status	Version	IAM Role
networking	Active	v1.24.7-eksbuild.2	Inherited from node

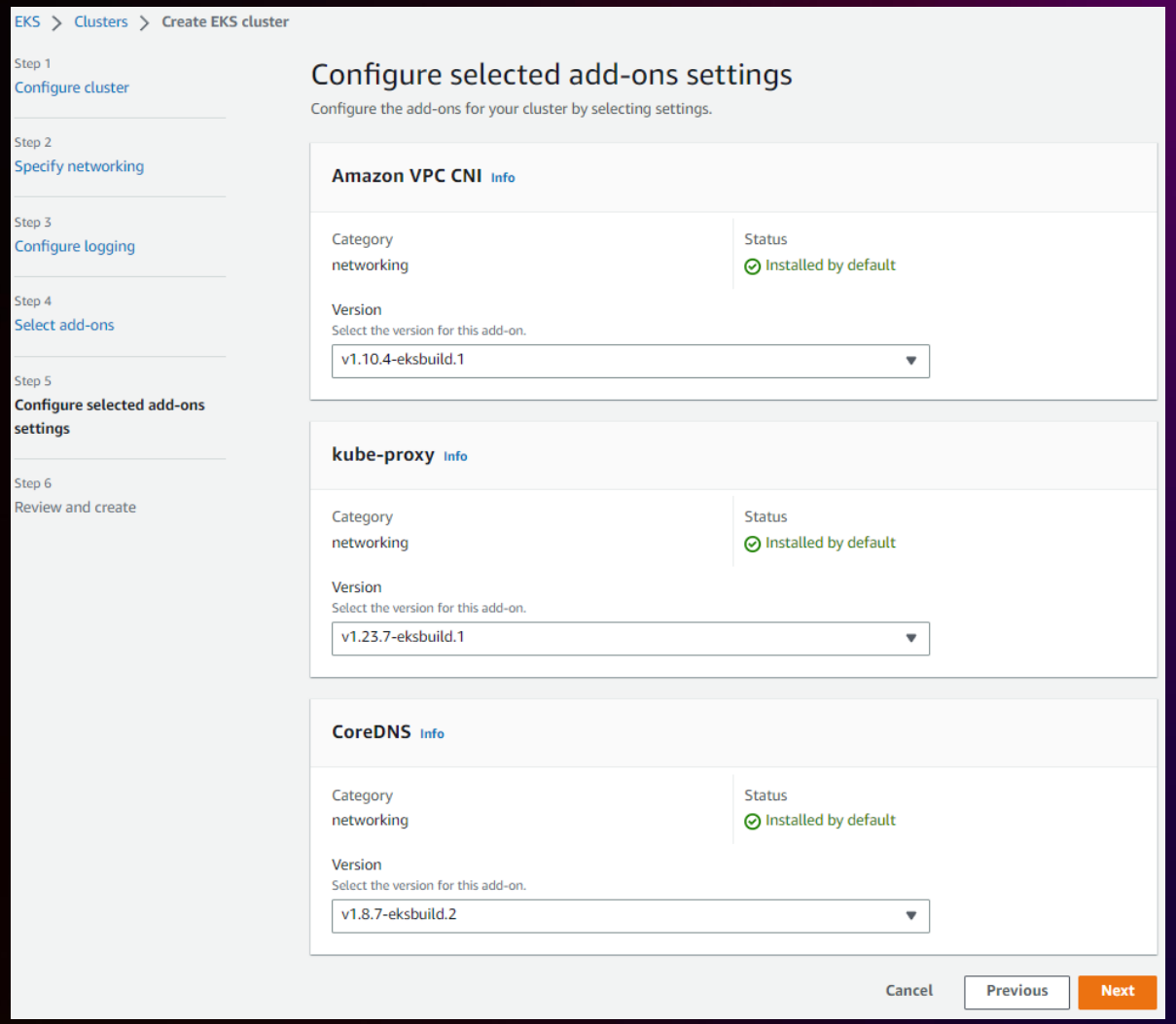
Amazon VPC CNI
Enable pod networking within your cluster.

Category	Status	Version	IAM Role
networking	Active	v1.11.4-eksbuild.1	Inherited from node

Update version

Amazon EKS add-ons creation during cluster creation

- Version selection during cluster creation
- Inherits IAM role of the node, can be updated later



Amazon EKS add-ons creation, any time

EKS > Clusters > addons-demo

addons-demo

Delete cluster

Cluster info Info

Kubernetes version Info	Status	Provider
1.24	Active	EKS

Overview | Resources | Compute | Networking | Add-ons | Authentication | Logging | Update history | Tags

Add-ons (3) Info

View details | Edit | Remove | Get more add-ons

Find add-on | Any category | Any status

1

CoreDNS
Enable service discovery within your cluster.

Category	Status	Version	IAM Role
networking	Active	v1.8.7-eksbuild.3	Inherited from node

kube-proxy
Enable service networking within your cluster.

Category	Status	Version	IAM Role
networking	Active	v1.24.7-eksbuild.2	Inherited from node

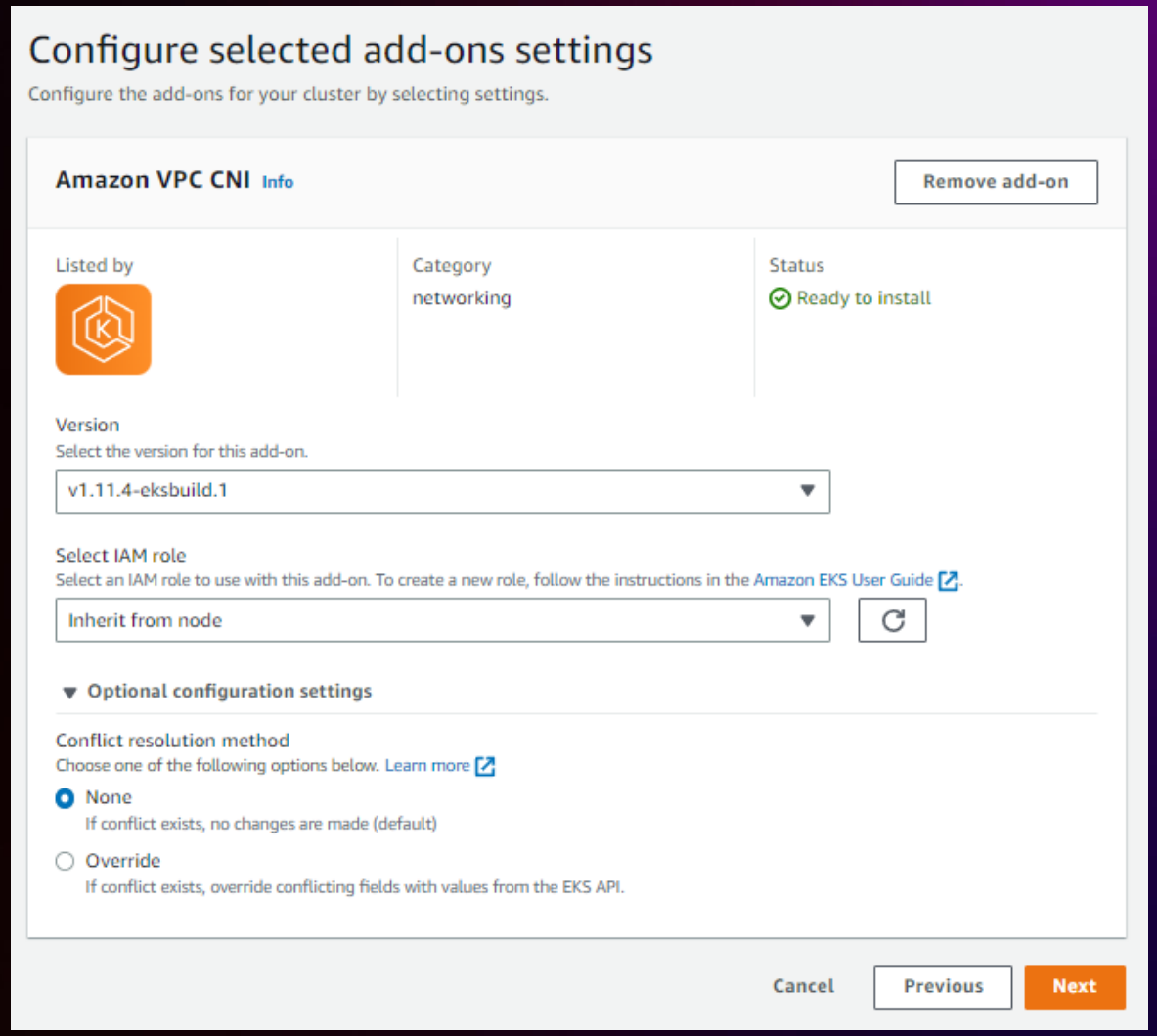
Amazon VPC CNI
Enable pod networking within your cluster.

Category	Status	Version	IAM Role
networking	Active	v1.11.4-eksbuild.1	Inherited from node

Update version

Amazon EKS add-ons creation, any time

- Selection for add-on type and version
- Choose to inherit node role or specify a custom role



Single-operation updates

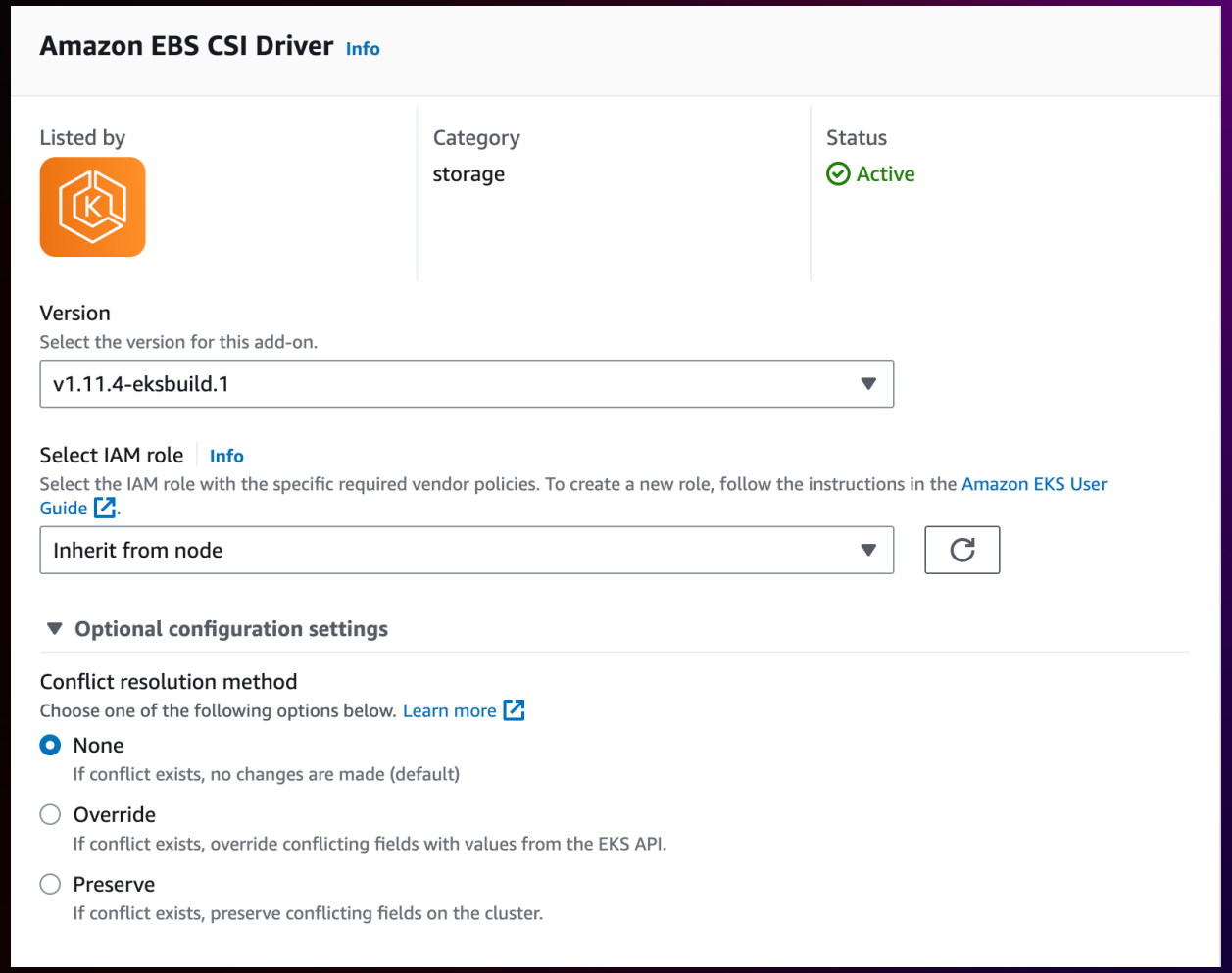
- Single-operation updates and role changes
- Rolling updates, no outages
- Configuration customization is preserved
- Optionally resolve conflicts during upgrade

Lifecycle management & custom configuration

- Amazon EKS add-ons use the new server-side apply feature in Kubernetes (v1.18)
- New merging algorithm as well as tracking of field ownership and changes over time
- Results in server-side reporting of configuration conflicts and improved conflict resolution
- Add-on configuration customization is preserved across lifecycle management operations

Amazon EKS add-ons updates

- Select desired version from the drop down
- Choose to inherit node role or specify a custom one
- Optionally override or preserve existing configuration if there are conflicts



Amazon EKS add-ons updates

- Kubernetes objects are gracefully cycled
- Add-on is active at its new version once complete

```
Events:
  Type    Reason            Age    From                  Message
  ----    ------            ----   ----                  -------
  Normal  SuccessfulDelete  17m    daemonset-controller  Deleted pod: aws-node-vxqrb
  Normal  SuccessfulCreate  17m    daemonset-controller  Created pod: aws-node-27w8f
  Normal  SuccessfulDelete  16m    daemonset-controller  Deleted pod: aws-node-ndx7f
  Normal  SuccessfulCreate  16m    daemonset-controller  Created pod: aws-node-gcj5m
  Normal  SuccessfulDelete  15m    daemonset-controller  Deleted pod: aws-node-vdvbr
```

Amazon EBS CSI Driver

Enable Amazon Elastic Block Storage (EBS) within your cluster

Category	Status	Version	IAM Role
storage	Active	v1.12.1-eksbuild.2	Inherited from node

Update version

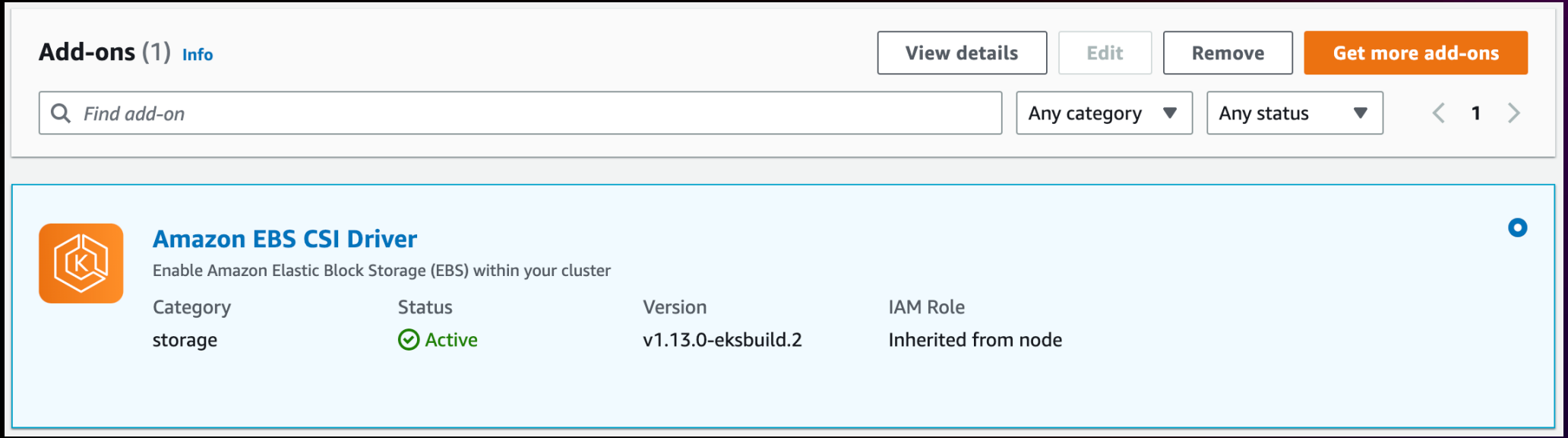
Amazon EBS CSI Driver

Enable Amazon Elastic Block Storage (EBS) within your cluster

Category	Status	Version	IAM Role
storage	Updating	v1.11.4-eksbuild.1	Inherited from node

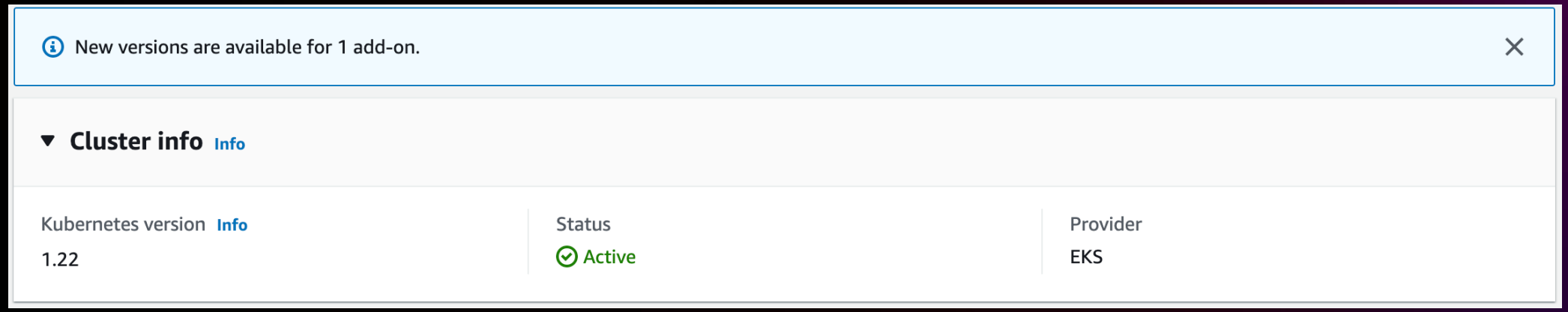
Amazon EKS add-ons updates

- Edit add-on at any time to its modify version
- Down-rev add-ons have an “Update now” action



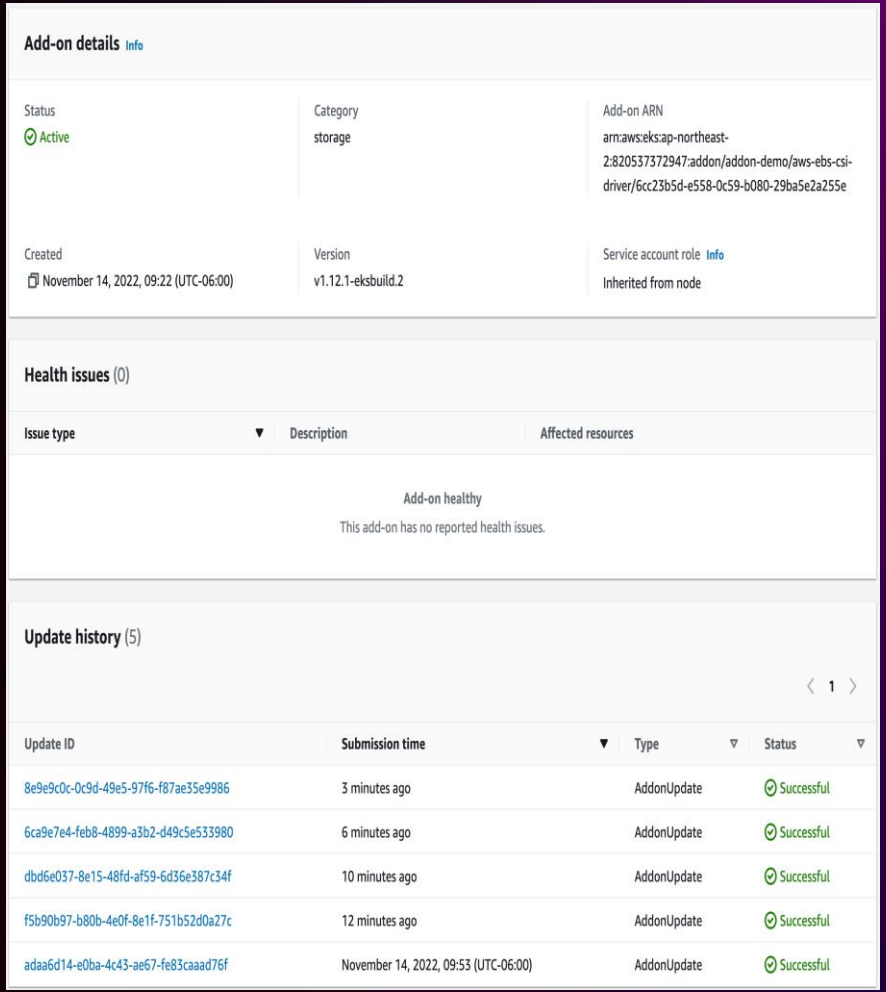
Amazon EKS add-ons updates

Additionally, down-rev add-ons are seen in a banner



Amazon EKS add-ons updates

- As with cluster and node group updates, full update history is available
- Each update entry has detailed information, such as version, state, and conflicts resolved



Amazon EKS add-ons with the AWS CLI

Of course, if you prefer **AWS CLI**, there are new commands

```
$ aws eks list-addons --cluster-name eks-luna
$ aws eks create-addon --cluster-name eks-luna --addon-name vpc-cni --addon-version 1.6.3
$ aws eks describe-addon --cluster-name eks-luna --addon-name vpc-cni
$ aws eks update-addon --cluster-name eks-luna --addon-name vpc-cni --addon-version 1.7.5
```

Optionally provide service account ARN, default inherits

Optionally resolve conflicts by overriding or preserving configuration

Amazon EKS add-ons with eksctl

Also, support in **eksctl**

```
$ eksctl get addons --cluster eks-molly
$ eksctl create addon --name vpc-cni --version 1.6.5 --cluster eks-molly
$ eksctl update addon --name vpc-cni -version 1.7.4 --cluster eks-molly
```

Optionally provide service account ARN, default inherits

Optionally override configuration and resolve conflicts

Amazon EKS add-ons with eksctl

```
$ eksctl create cluster -f config.yaml

apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
  name: basic-cluster
  region: eu-north-1

iam:
  withOIDC: true

addons:
  - name: vpc-cni
    version: 1.7.5
    serviceAccountRoleARN: role-arn
```

If `withOIDC` is true without a policy specified, a role will be created for the add-on with the required policy

Recent updates

New add-ons

Amazon EBS CSI driver
https://docs.aws.amazon.com/eks/latest/userguide/ebs-csi.html

AWS Distro for OpenTelemetry
https://aws.amazon.com/otel/

Preserving customer edits

Issue

- Changes made through the Kubernetes API after add-on creation were overwritten by the automated drift-prevention process (15 minutes)

Resolution

- Add-ons no longer overwrite settings during steady-state operations

The only time that add-ons will overwrite configuration is during create, update, and delete operations

Resolve conflict option

- A new ResolveConflicts option, **PRESERVE**, has been added to the Amazon EKS API: https://docs.aws.amazon.com/eks/
- Preserves any in-cluster configuration that was made through Kubernetes API

```
aws eks update-addon --cluster-name <CLUSTER_NAME> --addon-name coredns
--addon-version v1.8.5-eksbuild.1 --resolve-conflicts PRESERVE
```

Using OVERWRITE to resolve conflicts

Issue

- If you create or update a managed add-on after editing a field that is or will be managed by an add-on, conflicts cause the operation to fail

Resolution

- Use the **OVERWRITE** or **PRESERVE** options with create operations

```
aws eks create-addon --cluster-name <CLUSTER_NAME> --addon-name
kube-proxy --resolve-conflicts OVERWRITE
```

Preserve Kubernetes resources beyond deletion

You can delete the add-on and choose whether or not to retain the underlying Kubernetes resources

```
aws eks delete-addon --cluster-name <CLUSTER_NAME> --addon-name <ADDON_NAME> --preserve
```

Introducing AWS Marketplace integration for Amazon EKS add-ons

Add-on workflow: Before

- Google search
- Vendor website
- Personal recommendation
- Marketplace

- Free trial/demo
- Tech evaluation
- Architecture review
- Security analysis
- Review pricing
- Review contracts

- Request to purchase
- Sign contract/terms
- Review optional private offer
- Purchase/subscribe

- Scan for vulnerabilities
- Obtain credentials
- Configure
- Cost optimization
- Deploy

- Manage usage performance
- Manage relationships
- Scan images for vulnerabilities
- License renewals
- Receive and pay invoices

Add-on workflow: AWS Marketplace integration

- Discover in AWS Marketplace catalog or Amazon EKS console

- AWS Marketplace only presents compatible and trusted software

- Initiate the procurement process from Amazon EKS console and complete steps in AWS Marketplace

- Amazon EKS scans marketplace software for vulnerabilities
- Easy install in UI or commands in other environments

- Finds updates and notifies customer
- Configuration in UI

What is AWS Marketplace integration?

- Find and subscribe to third party Kubernetes add-ons from AWS Marketplace through the Amazon EKS console
- Deploy those add-ons using AWS APIs, eksctl, and other infrastructure as code (IaC) tools including AWS CloudFormation and Terraform
- Software is continually scanned for common vulnerabilities and exposures (CVEs), and are validated by AWS to work with Amazon EKS
- Customers are presented with add-on versions that are compatible with their Kubernetes version
- Post deployment, customers will receive notifications when new versions are available to upgrade and ensure they are running the latest patches at all times

How to subscribe

- Subscriptions are managed through AWS Marketplace
- Use AWS License Manager to automate the distribution and activation of software entitlements to end users and workloads; entitlements provide built-in controls that allow only approved users and workloads to consume licenses

How to enable/deploy

- Accept the software price
- Accept the end user license agreement (EULA)
- Select the version of the software you would like to deploy

Note: You will need to subscribe to the commercial add-ons before you can deploy them on Amazon EKS clusters

New version notifications

- Banner in the Amazon EKS console
- In the case a CVE is detected, AWS will notify you to deploy the latest compatible version of the software to your clusters; these notifications will be made through an Amazon SNS notification by AWS Marketplace and Amazon EKS APIs

Third-party catalog on Amazon EKS powered by AWS Marketplace

Launch partners

kubecost
upbound
Tetrate Istio Subscription
Teleport
dynatrace
factor house
engineering insights

Coming soon

new relic
nOps
Lightrun
Shoreline
RAFAY
DATADOG
NeuVector
Full Lifecycle Container Security
Kong
paloalto NETWORKS
TRILIO
StormForge
sysdig
kasten by Veeam
PARALUS
datree
LACEWORK
portworx
nirmata
DataStax
AEROSPIKE
HAPROXY

This is not a complete list. To view all AWS Partners for this category, visit AWS Partner Solutions Finder.
This list of partners is current as of November 28, 2022.

Best practices

Add-on best practices

- Use them
- Decide whether you're going to use the Amazon EKS API or the Kubernetes API to manage the add-ons settings
- Use **PRESEVE** option to preserve changes made through the Kubernetes API
- Use `describe-addon` to view conflicts
- Use **OVERWRITE** option to reset addon to known good configuration

Connect with us

- As always, our work is guided by you
- Visit the AWS container services roadmap on GitHub

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

Thank you!

Jeremy Cowan

Sriram Ranganathan

www.linkedin.com/in/sriramranga

Please complete the session survey in the **mobile app**