
AWS
re:Invent
DECEMBER 2 – 6, 2024 | LAS VEGAS, NV

KUB205-NEW

# Bring the power of Amazon EKS to your on-premises applications

**Chris Splinter**
Principal Product Mgr., Kubernetes
AWS

**Jonathan Ogden**
Sr. Director, Engineering
Northwestern Mutual

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Agenda

01 Kubernetes on-premises challenges

02 Amazon EKS hybrid/edge overview

03 🚀 Amazon EKS Hybrid Nodes 🚀

04 Northwestern Mutual use case

05 Q&A

aws

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Kubernetes on-premises challenges

Operational overhead

Long-term commitments

Limited experience

Technology sprawl

Difficult to make changes

Complex to scale

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Our goals for AWS Kubernetes

**Simplify** **Supercharge** **Standardize**

Application-ready production Kubernetes
in the cloud and data center

**What this means for you**

Focus on your expertise

Reliable systems at scale

Consistency across environments

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS hybrid/edge overview

## Cloud-connected use cases

Amazon EKS on AWS Outposts

2019

Enterprise modernization

Local data processing

**AWS-MANAGED KUBERNETES CONTROL PLANE**

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS hybrid/edge overview

## Cloud-connected use cases

Amazon EKS on AWS Outposts

2019

Enterprise modernization

Local data processing

## Cloud-disconnected use cases

Amazon EKS Anywhere

2021

Air-gapped environments

Telco

Financial services

Travel

**AWS-MANAGED KUBERNETES CONTROL PLANE**

**CUSTOMER-MANAGED CLUSTER OPERATIONS**

aws

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS Hybrid Nodes

BRING THE POWER OF AMAZON EKS TO YOUR ON-PREMISES APPLICATIONS

**Customers can now use existing on-premises and edge infrastructure as nodes in Amazon EKS clusters for unified Kubernetes management across environments**

- ✓ Improve operational efficiency by unifying Kubernetes operations across environments
- ✓ Reduce total cost of ownership of managing Kubernetes
- ✓ Get the benefits of AWS Cloud on premises
- ✓ Gain the flexibility to run your workloads anywhere

aws

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS hybrid/edge overview

## Cloud-connected use cases

Amazon EKS on AWS Outposts

2019

Amazon EKS Hybrid Nodes

NEW

Enterprise modernization

Local data processing

Machine learning

Manufacturing

**AWS-MANAGED KUBERNETES CONTROL PLANE**

## Cloud-disconnected use cases

Amazon EKS Anywhere

2021

Air-gapped environments

Telco

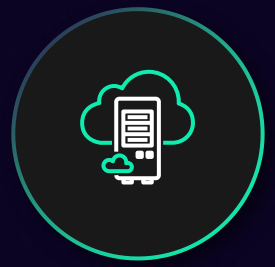
Financial services

Travel

**CUSTOMER-MANAGED CLUSTER OPERATIONS**

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS Hybrid Nodes use cases



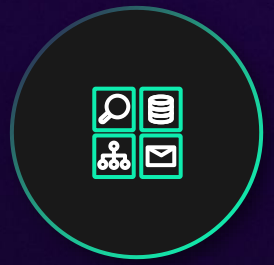
Enterprise modernization

Machine learning

Financial services

Media streaming

Manufacturing



Internal IT applications

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

“Amazon EKS Hybrid Nodes gives us an easy way to manage servers in our data centers.

We don’t need to leverage our own resources to run a Kubernetes cluster ourselves; we can now lean on Amazon Web Services (AWS) expertise to manage and maintain our control plane while remaining on premises for sensitive workloads.”

**Alex Smith**

Cloud Architect, Darktrace

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS Hybrid Nodes Validated Partners


Pulumi


spectro cloud


aqua


HashiCorp


CiQ


tetrate


SOLO.IO


PerfectScale


nirmata


New Relic.


NetApp


kubecost


Kong

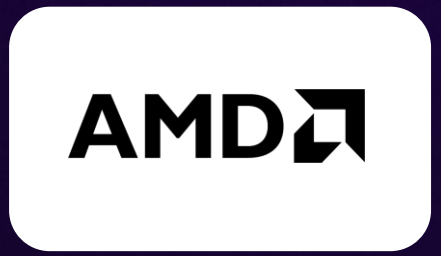

DELL Technologies


CONTINENT8 technologies


dynatrace


AccuKnox

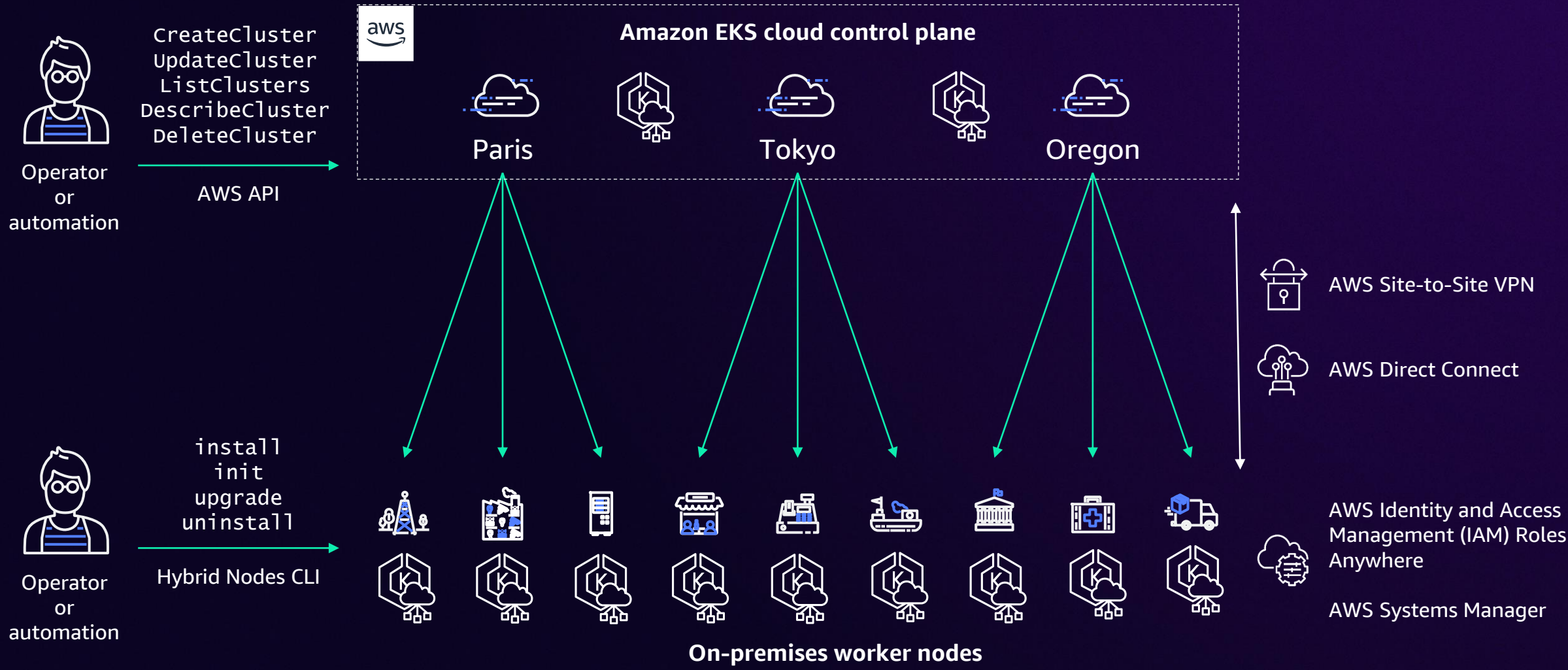

sysdig


AMD

aws

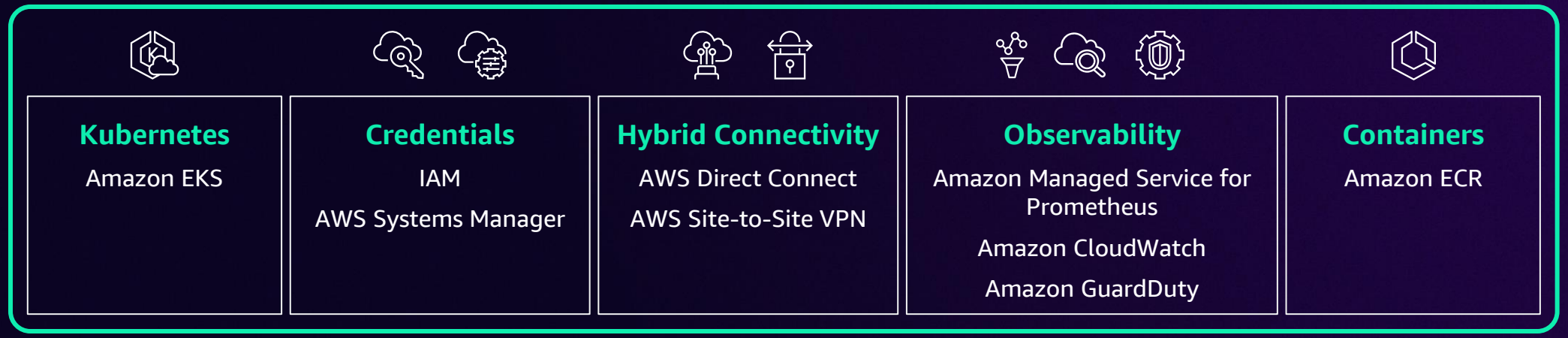
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

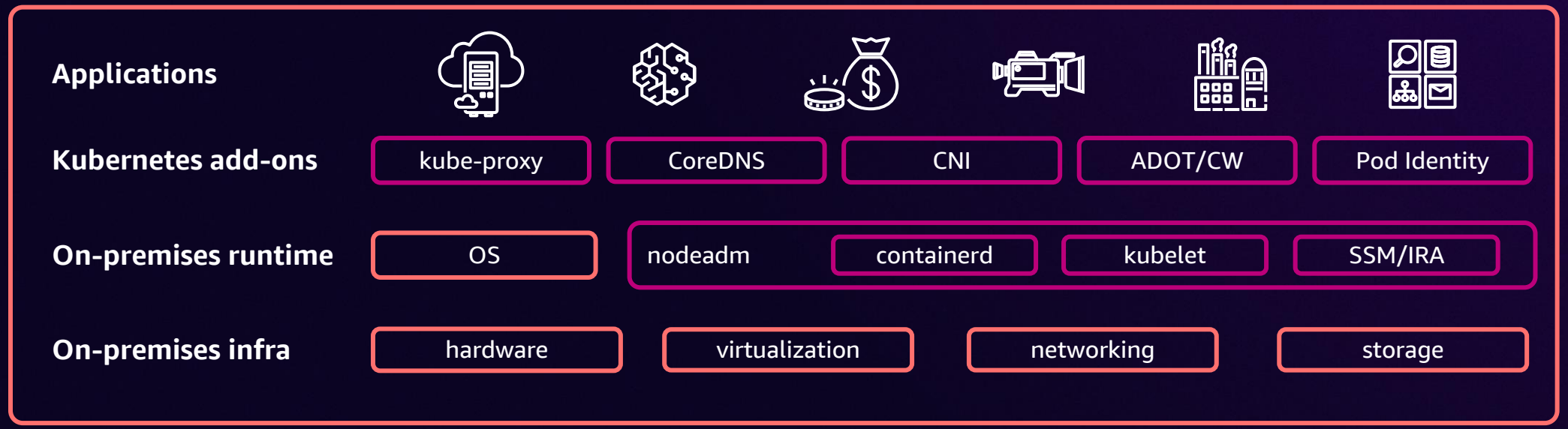
# Amazon EKS Hybrid Nodes architecture




© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS Hybrid Nodes shared responsibility







© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS Hybrid Nodes: How it works

## Network connectivity

AWS Site-to-Site VPN

AWS Direct Connect

## Infrastructure

Bare metal servers

Virtual machines

## Operating system

Ubuntu

Red Hat Enterprise Linux

Amazon Linux 2023

## Credential provider

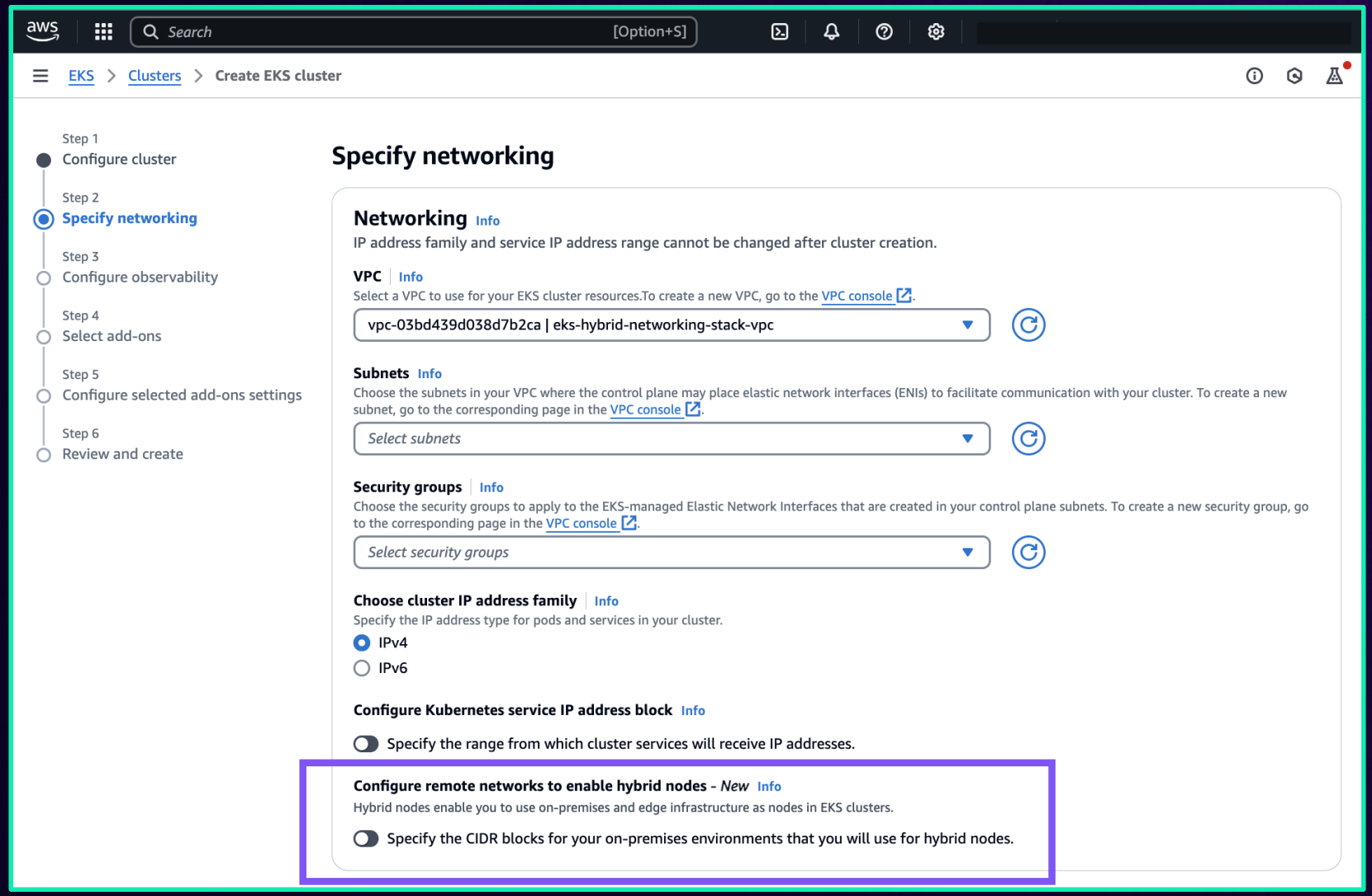
AWS Systems Manager

AWS IAM Roles Anywhere

aws

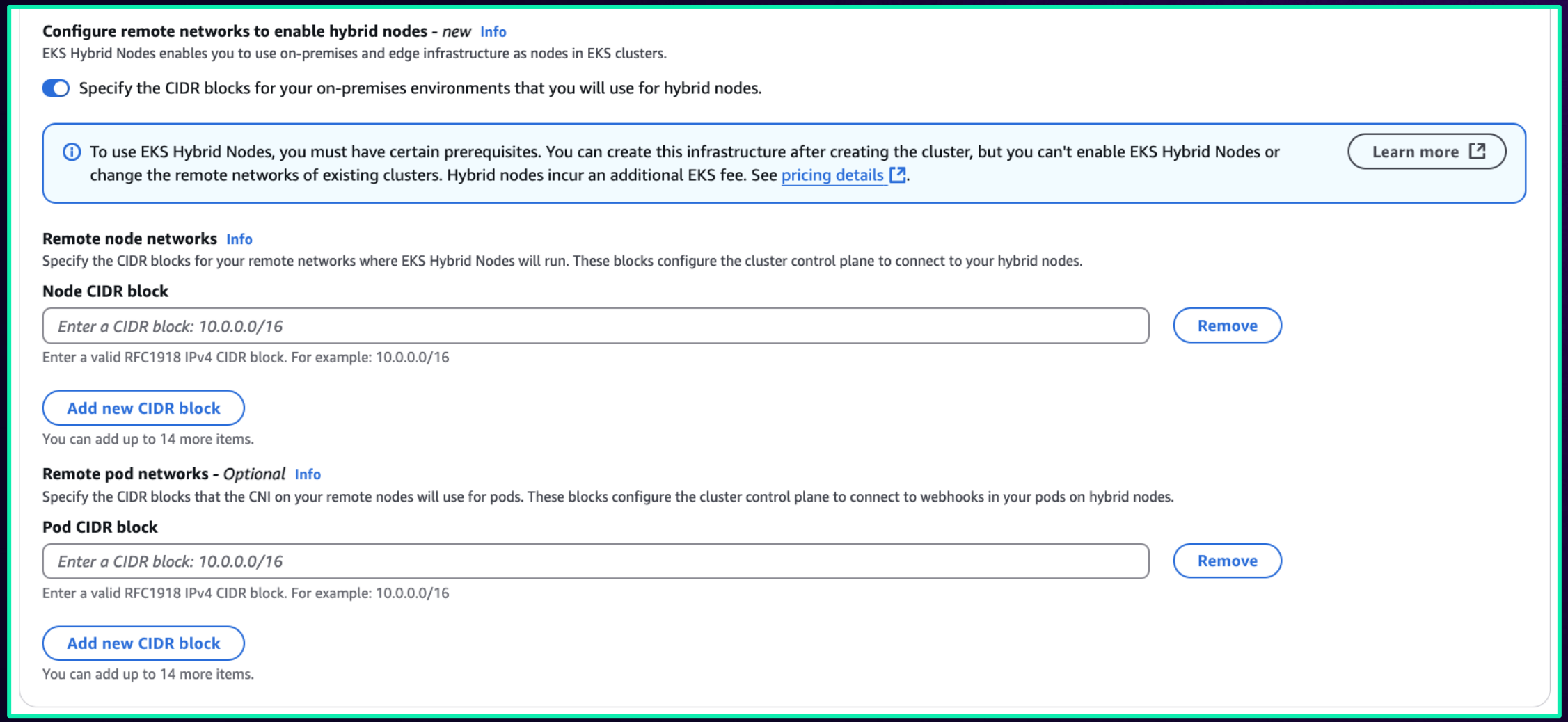
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS Hybrid Nodes: How it works




© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

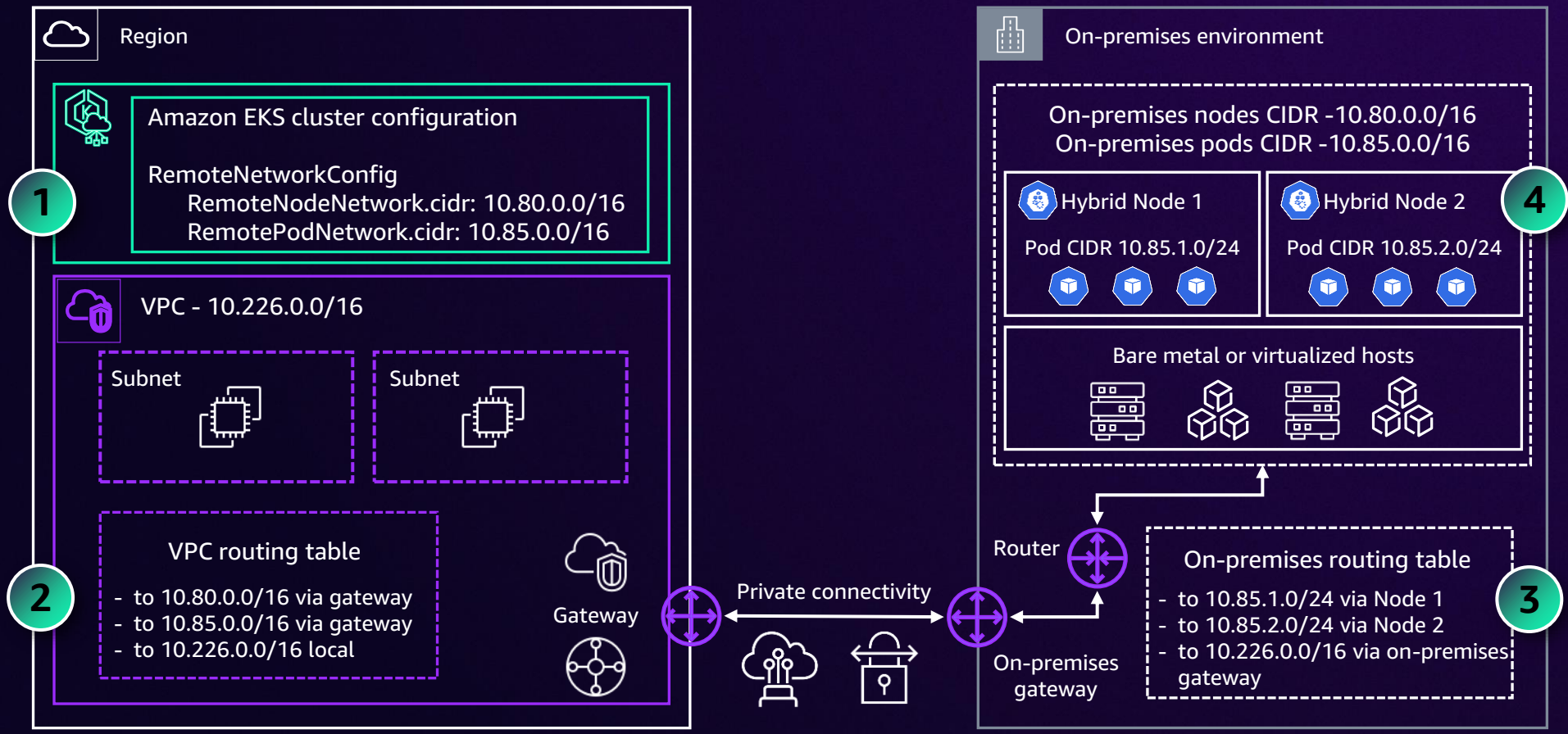
# Amazon EKS Hybrid Nodes: How it works




© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS Hybrid Nodes networking

1. Pass on-premises node and pod CIDRs in EKS cluster config
2. Configure VPC routes for on-premises node and pod CIDRs
3. Configure on-premises router with node and pod CIDR routes
4. Configure CNI with pod CIDR




© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS Hybrid Nodes networking

1. Private connectivity (AWS Direct Connect, AWS Site-to-Site VPN, your own VPN)
2. Reliable connectivity – at least 100 Mbps
3. Low latency, better experience – no greater than 200 ms round-trip latency

Network requirements vary by workload and environment

| | | |
|---|---|---|
| Number of nodes | Application size | Dependencies |
| Elasticity | Monitoring | Data access |

aws

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS Hybrid Nodes: How it works

**nodeadm**: hybrid nodes command-line interface (CLI)

- The hybrid nodes CLI is run on each on-premises host
- Simplifies installation, configuration, registration, upgrade, and uninstallation
- Include the CLI in your operating system images to automate node bootstrap
- Invoke the CLI as a systemd service or with tools such as Ansible at host startup

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS Hybrid Nodes: How it works

```
nodeadm init -c file://nodeConfig.yaml
```

AWS Systems Manager hybrid activations

```
apiVersion: node.eks.aws/v1alpha1
kind: NodeConfig
spec:
  cluster:
    name:              # EKS cluster name
    region:            # AWS Region
  hybrid:
    ssm:
      activationCode: # SSM hybrid activation code
      activationId:   # SSM hybrid activation id
```

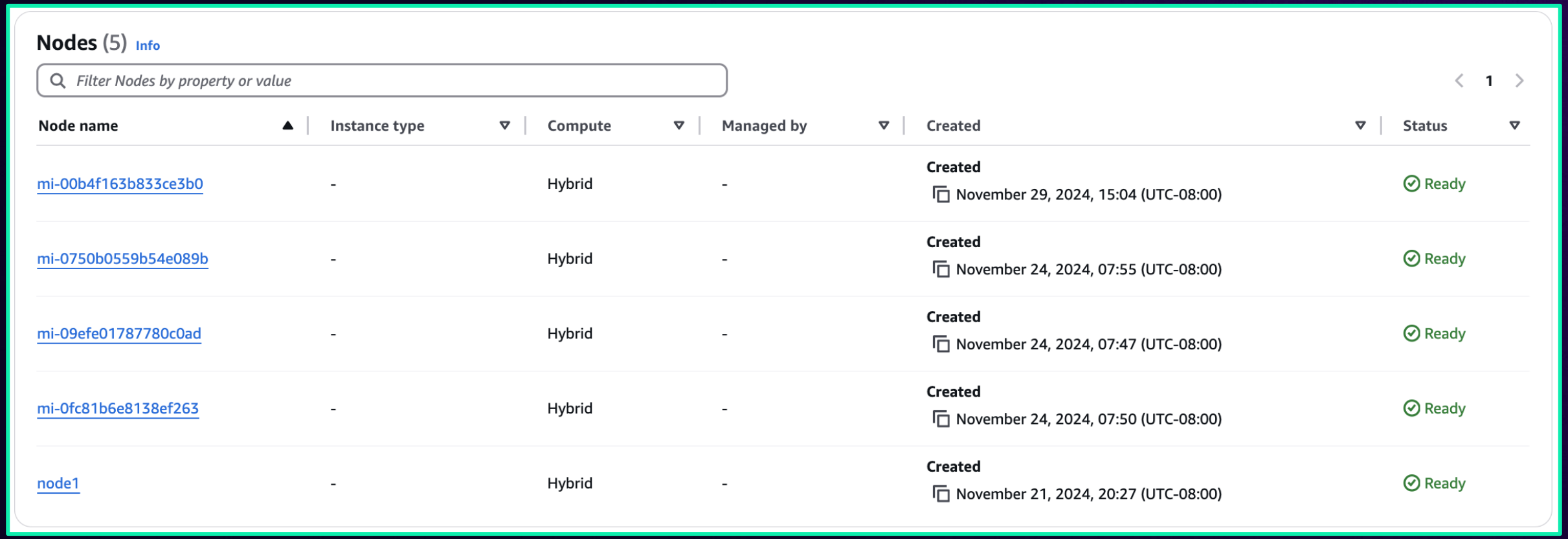
AWS IAM Roles Anywhere

```
apiVersion: node.eks.aws/v1alpha1
kind: NodeConfig
spec:
  cluster:
    name:              # EKS cluster name
    region:            # AWS Region
  hybrid:
    iamRolesAnywhere:
      nodeName:        # hybrid node name
      roleARN:         # hybrid node IAM role ARN
      trustAnchorArn: # IAM RA trust anchor ARN
      profileArn:      # IAM RA profile ARN
```

aws

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS Hybrid Nodes: How it works



**Nodes** (5) Info

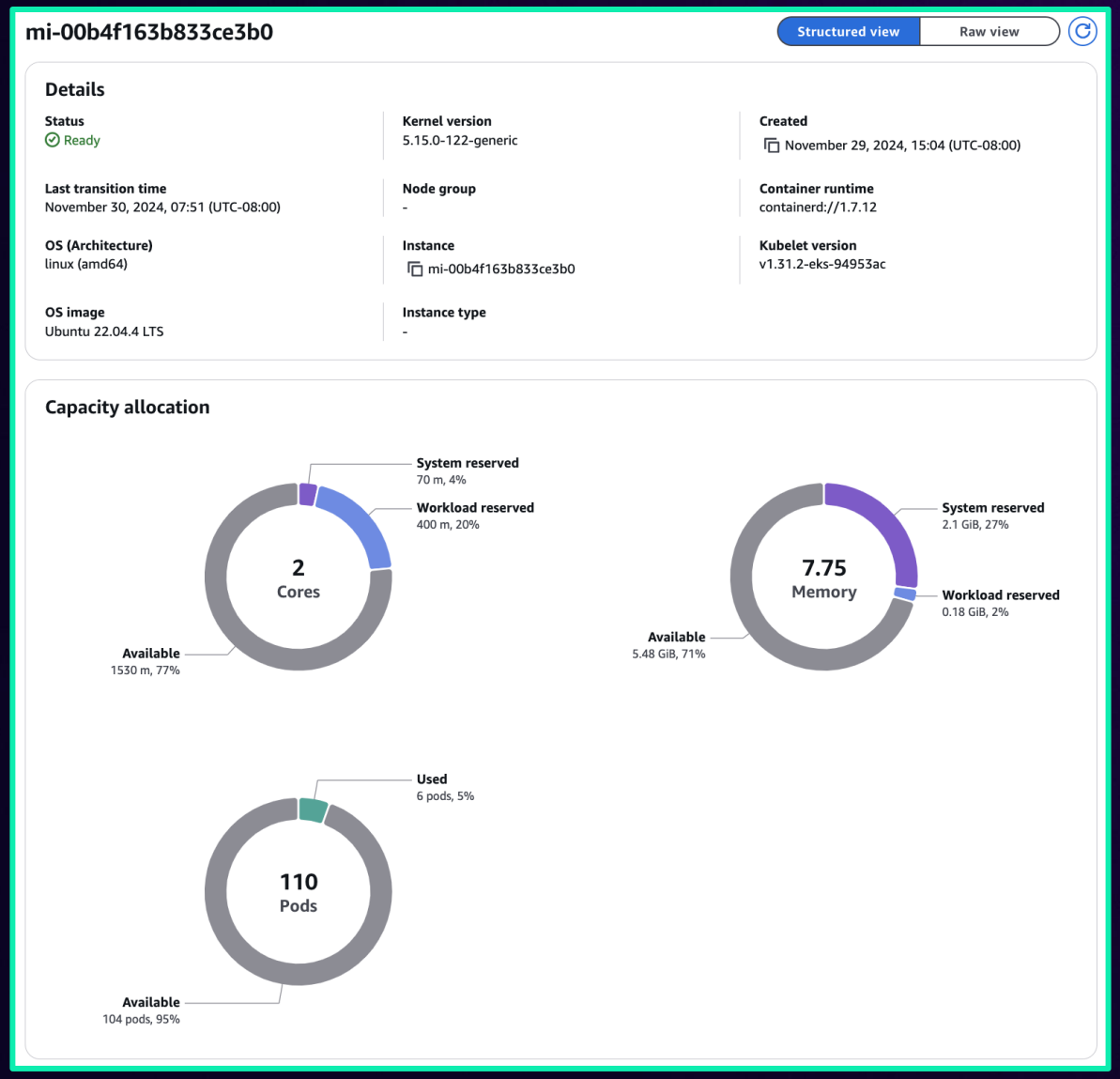
Filter Nodes by property or value

1

| Node name | Instance type | Compute | Managed by | Created | Status |
|---|---|---|---|---|---|
| mi-00b4f163b833ce3b0 | - | Hybrid | - | **Created** November 29, 2024, 15:04 (UTC-08:00) | Ready |
| mi-0750b0559b54e089b | - | Hybrid | - | **Created** November 24, 2024, 07:55 (UTC-08:00) | Ready |
| mi-09efe01787780c0ad | - | Hybrid | - | **Created** November 24, 2024, 07:47 (UTC-08:00) | Ready |
| mi-0fc81b6e8138ef263 | - | Hybrid | - | **Created** November 24, 2024, 07:50 (UTC-08:00) | Ready |
| node1 | - | Hybrid | - | **Created** November 21, 2024, 20:27 (UTC-08:00) | Ready |

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS Hybrid Nodes: How it works




© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS Hybrid Nodes features

Available in all AWS commercial regions

Available for new Amazon EKS clusters

Amazon EKS standard and extended Kubernetes versions

Amazon EKS console, CLI/SDKs, APIs, eksctl, AWS CloudFormation, Terraform

Amazon EKS cluster access entries (API, API_AND_CONFIG_MAP)

Mixed-mode clusters with hybrid nodes and cloud nodes

aws

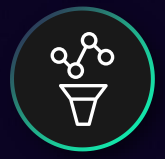
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS Hybrid Nodes features

IPv4 on-premises nodes with Cilium and Calico pod networking

CoreDNS add-on and auto-scaling, kube-proxy add-on

Amazon EKS Pod Identity and IAM roles for service accounts (IRSA)



Amazon Managed Service for Prometheus agentless metrics
and AWS Distro for OpenTelemetry add-on

Amazon CloudWatch control plane logging and CloudWatch Observability agent

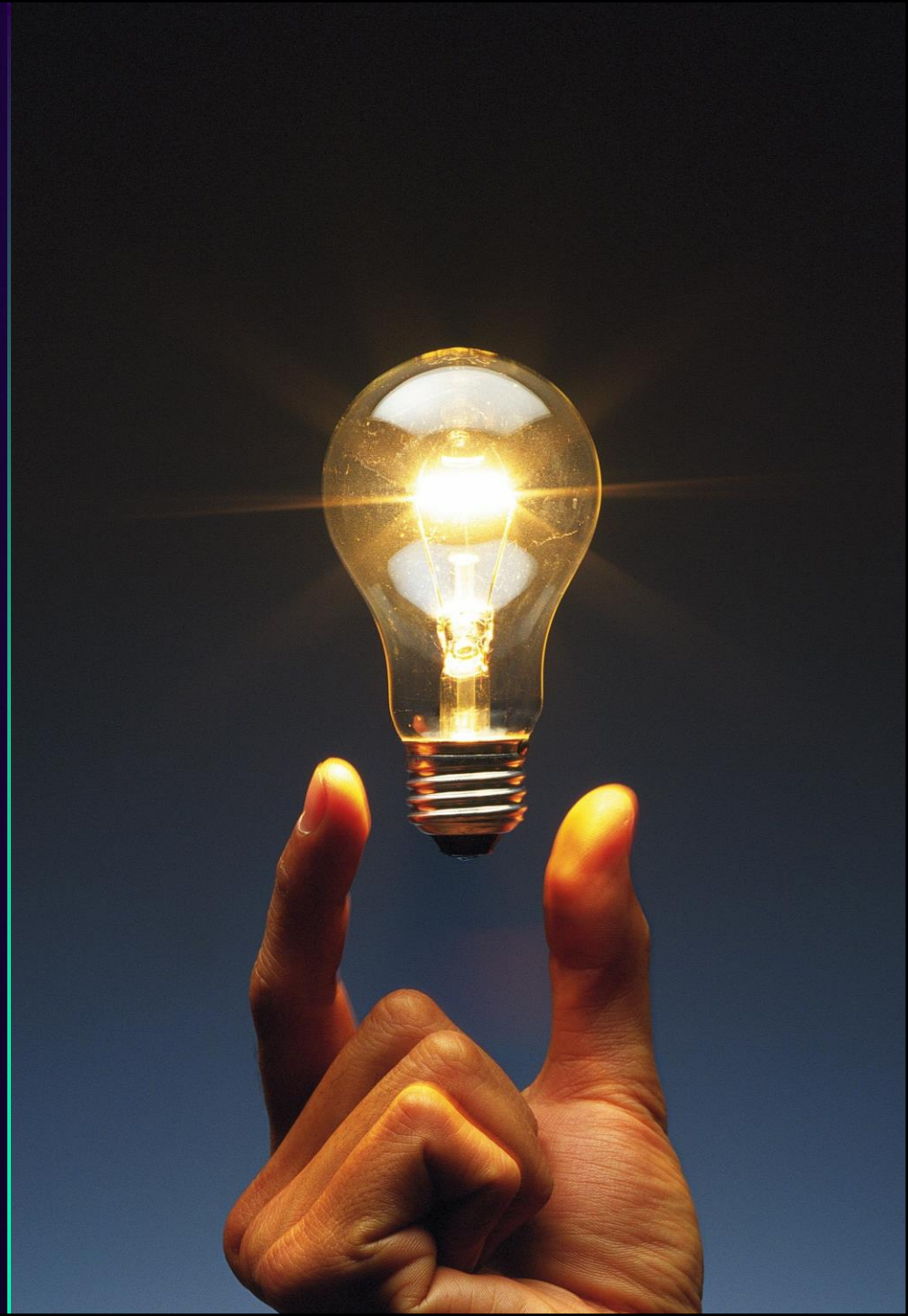
Amazon GuardDuty audit log monitoring

aws

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS Hybrid Nodes best practices

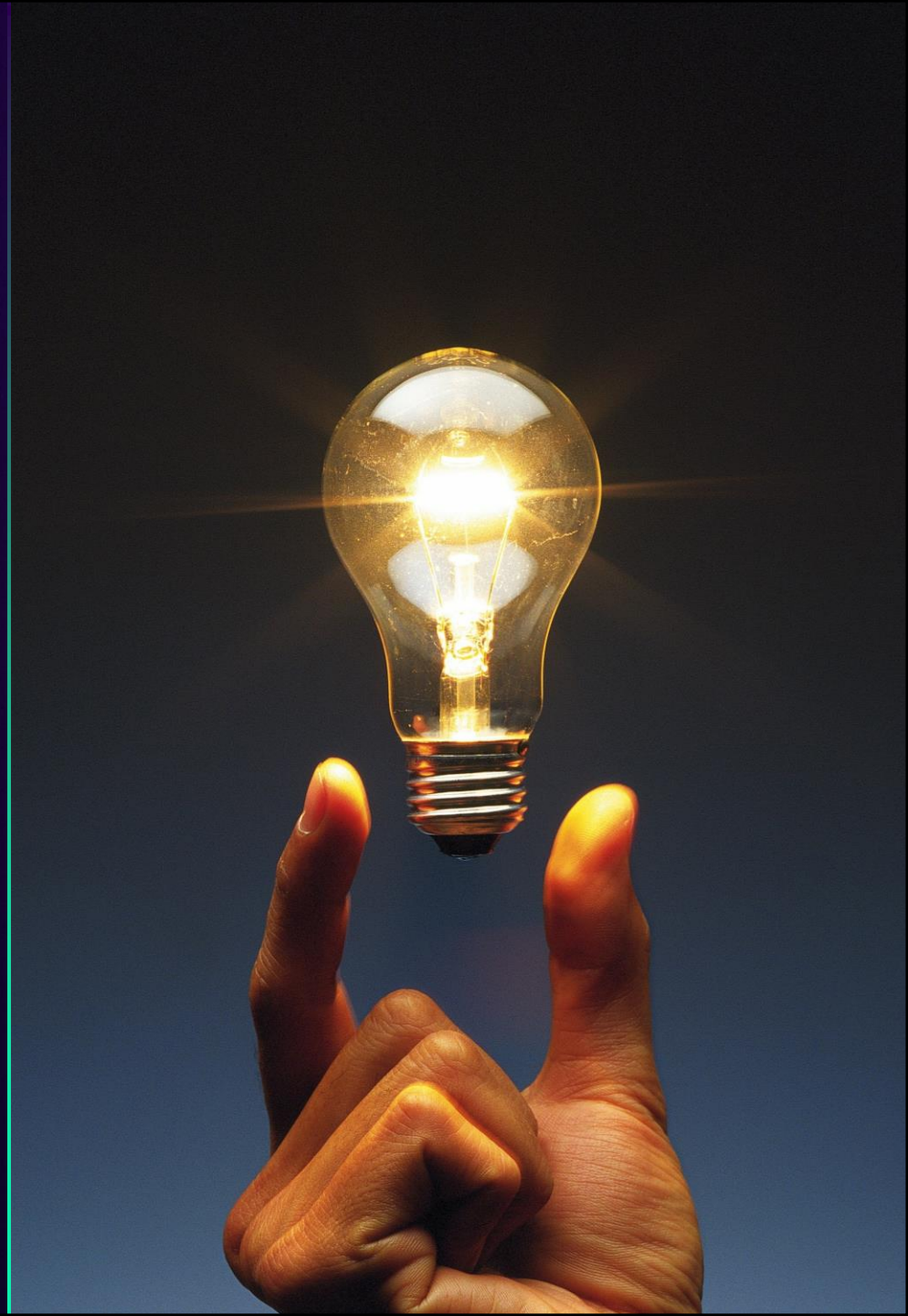
1
2
3
4
5



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS Hybrid Nodes best practices

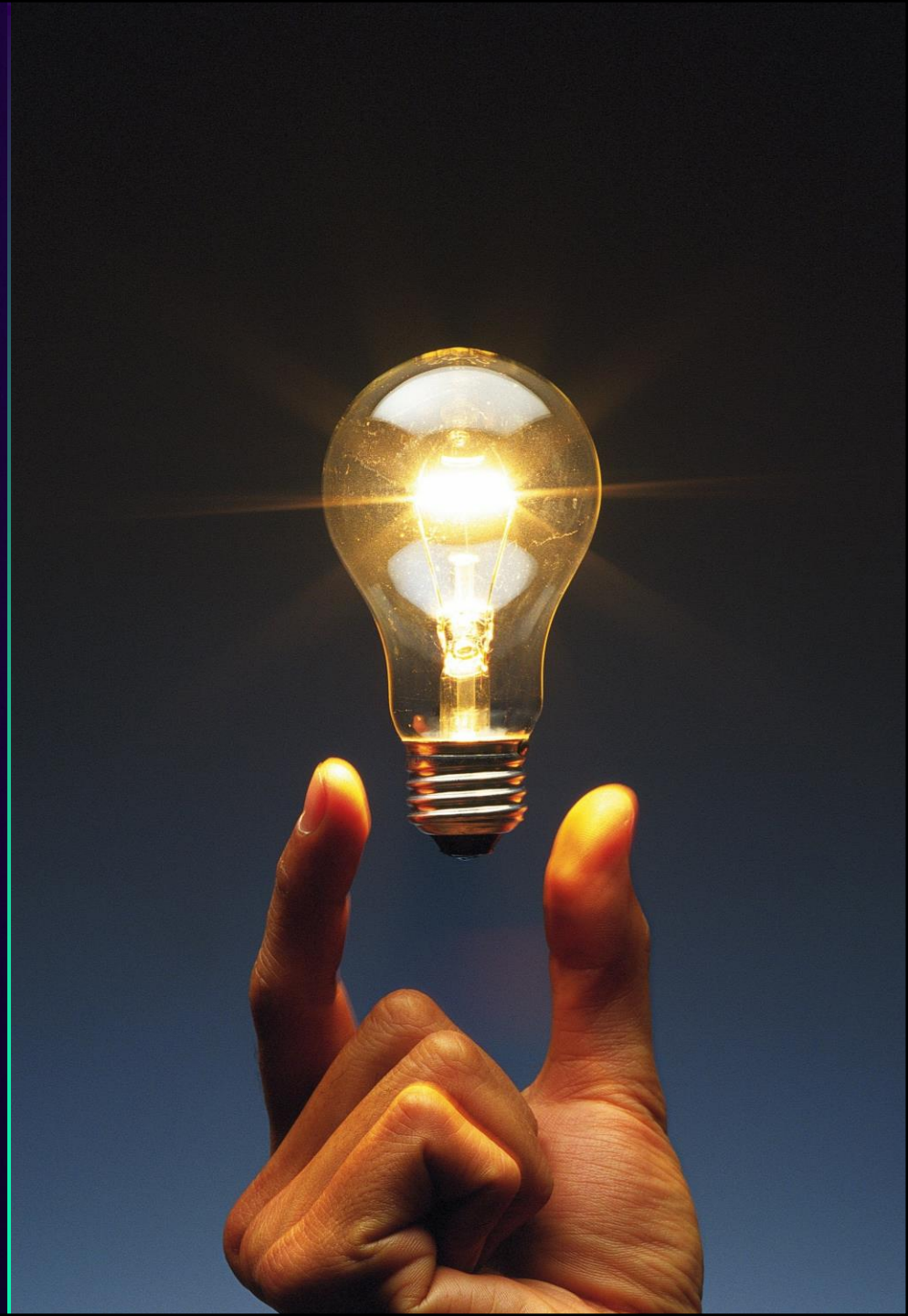
1. Automate node bootstrap
2. 
3. 
4. 
5. 



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS Hybrid Nodes best practices

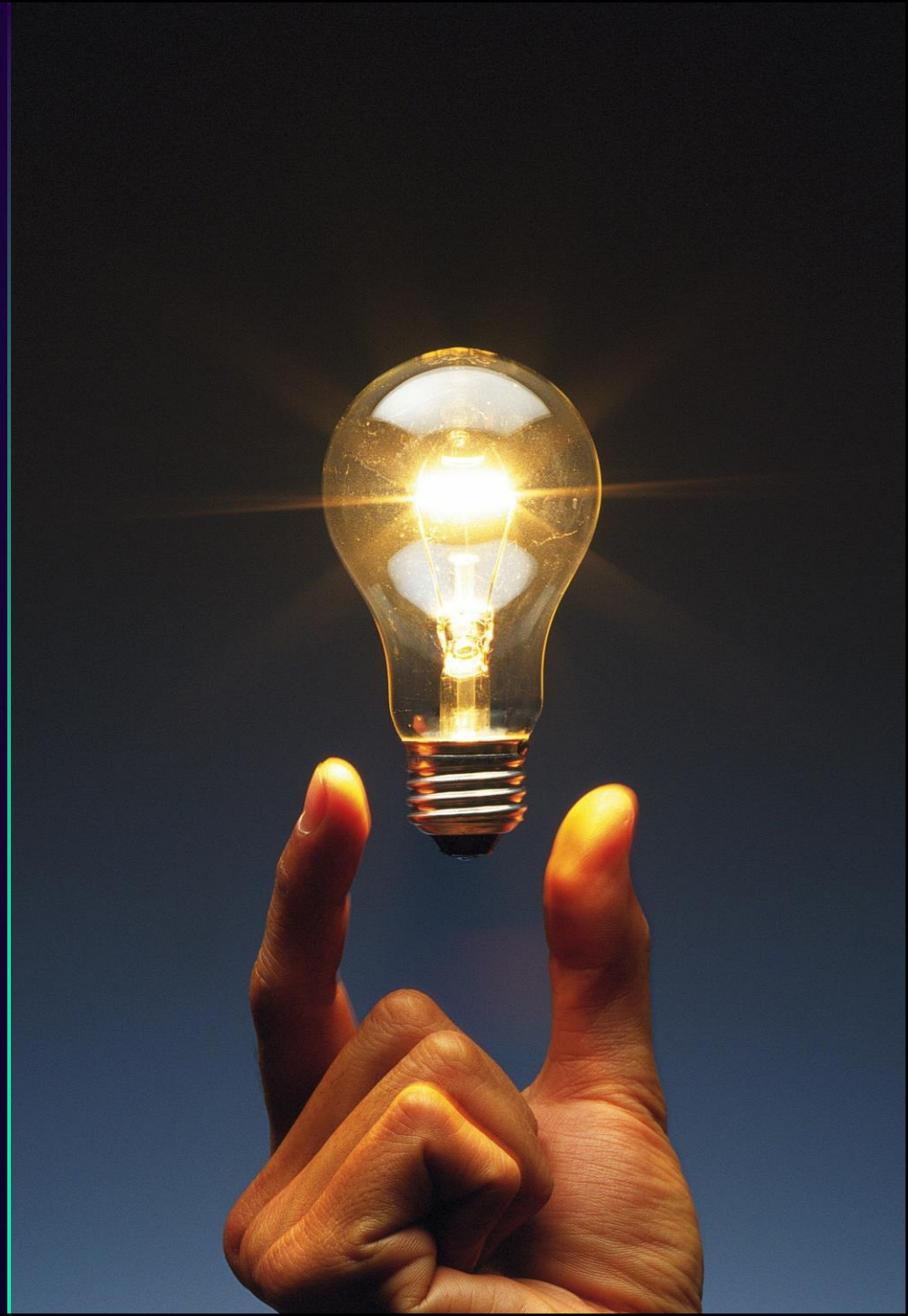
1. Automate node bootstrap
2. Use AWS Region closest to on-premises environment
3. 
4. 
5. 



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS Hybrid Nodes best practices

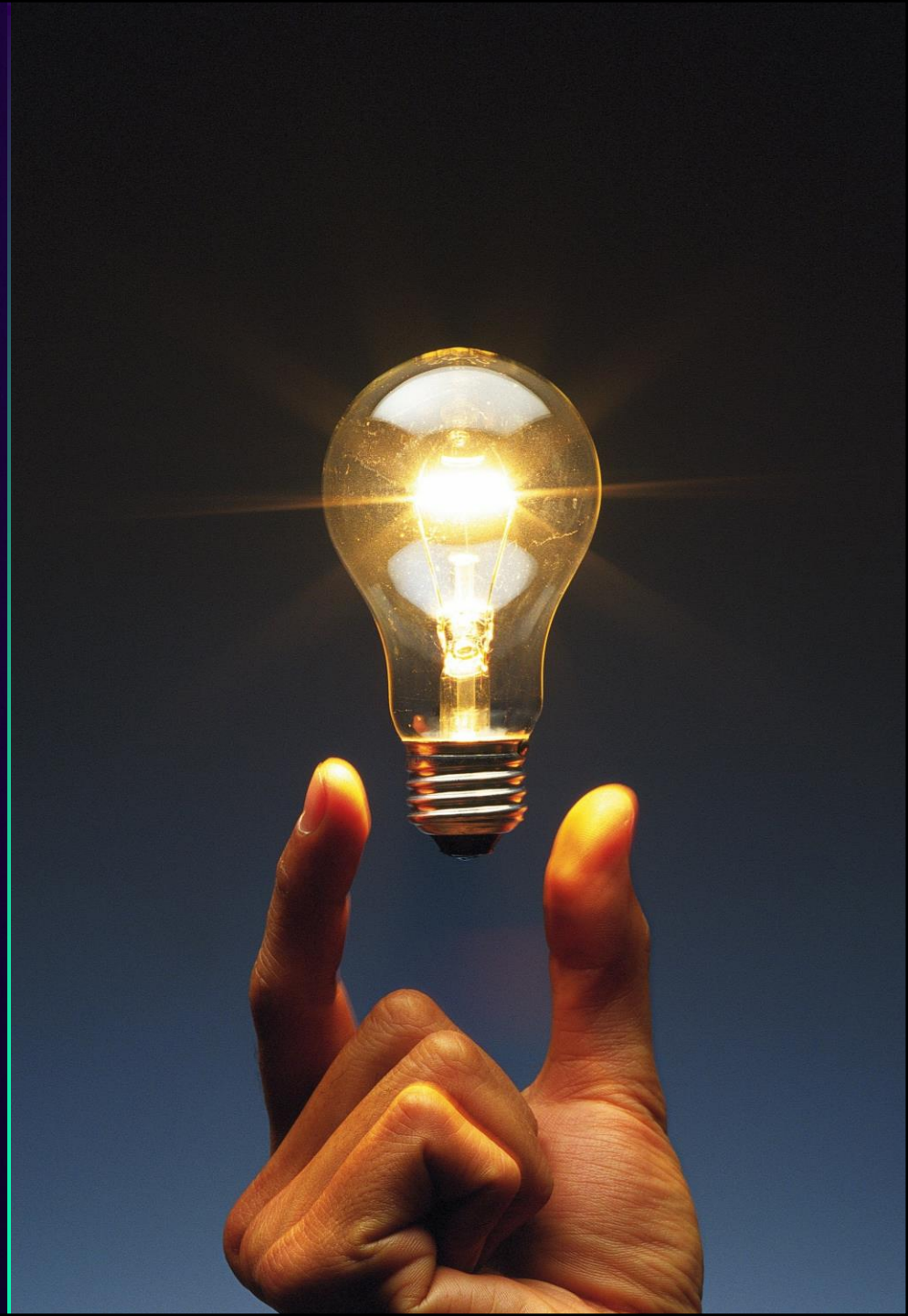
1. Automate node bootstrap
2. Use AWS Region closest to on-premises environment
3. Allow required endpoints/ports in firewall
4. 
5. 



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS Hybrid Nodes best practices

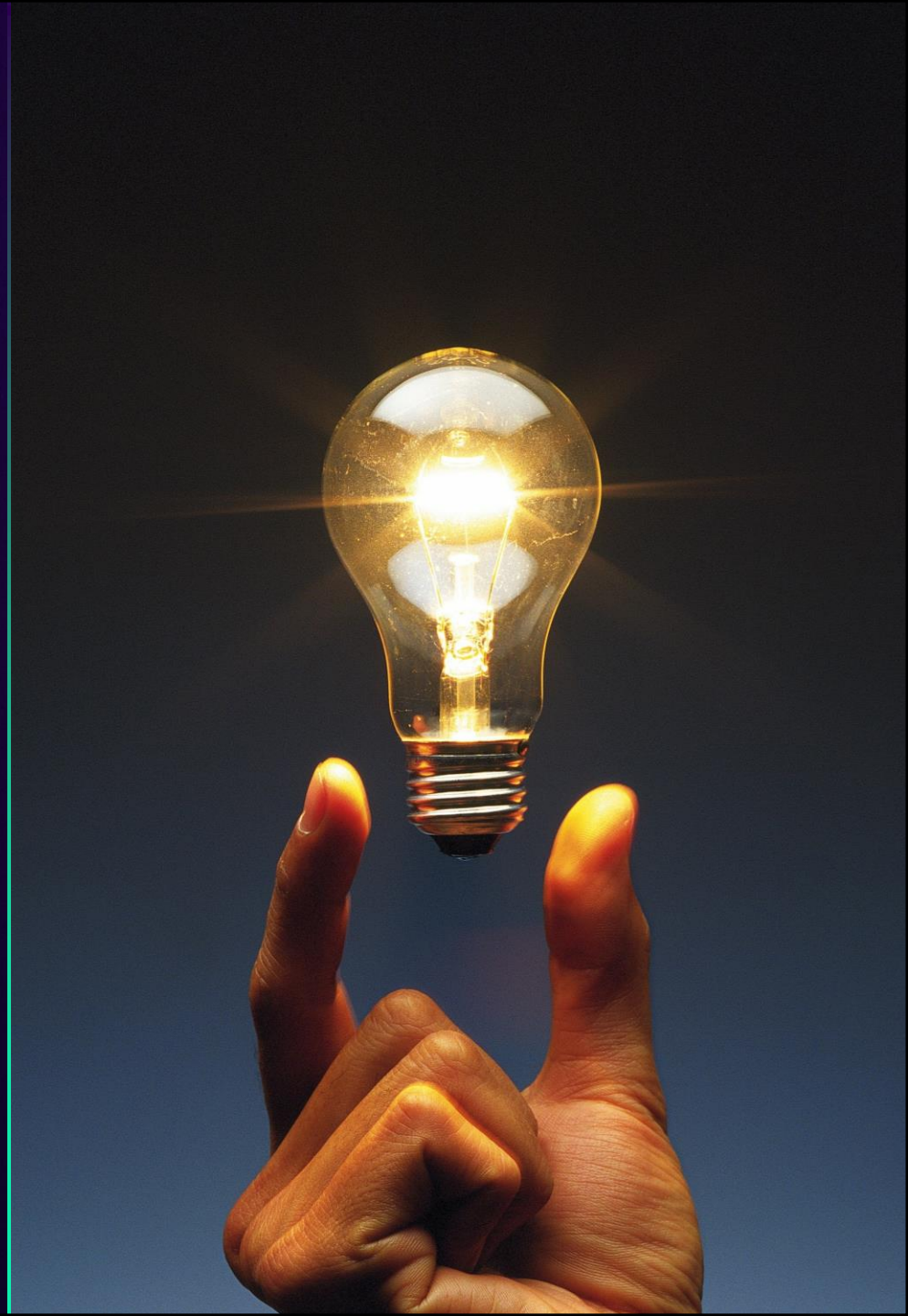
1. Automate node bootstrap
2. Use AWS Region closest to on-premises environment
3. Allow required endpoints/ports in firewall
4. Confirm VPC and on-premises routing
5.



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS Hybrid Nodes best practices

1. Automate node bootstrap
2. Use AWS Region closest to on-premises environment
3. Allow required endpoints/ports in firewall
4. Confirm VPC and on-premises routing
5. Affinity/anti-affinity for workload placement



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS Hybrid Nodes best practices

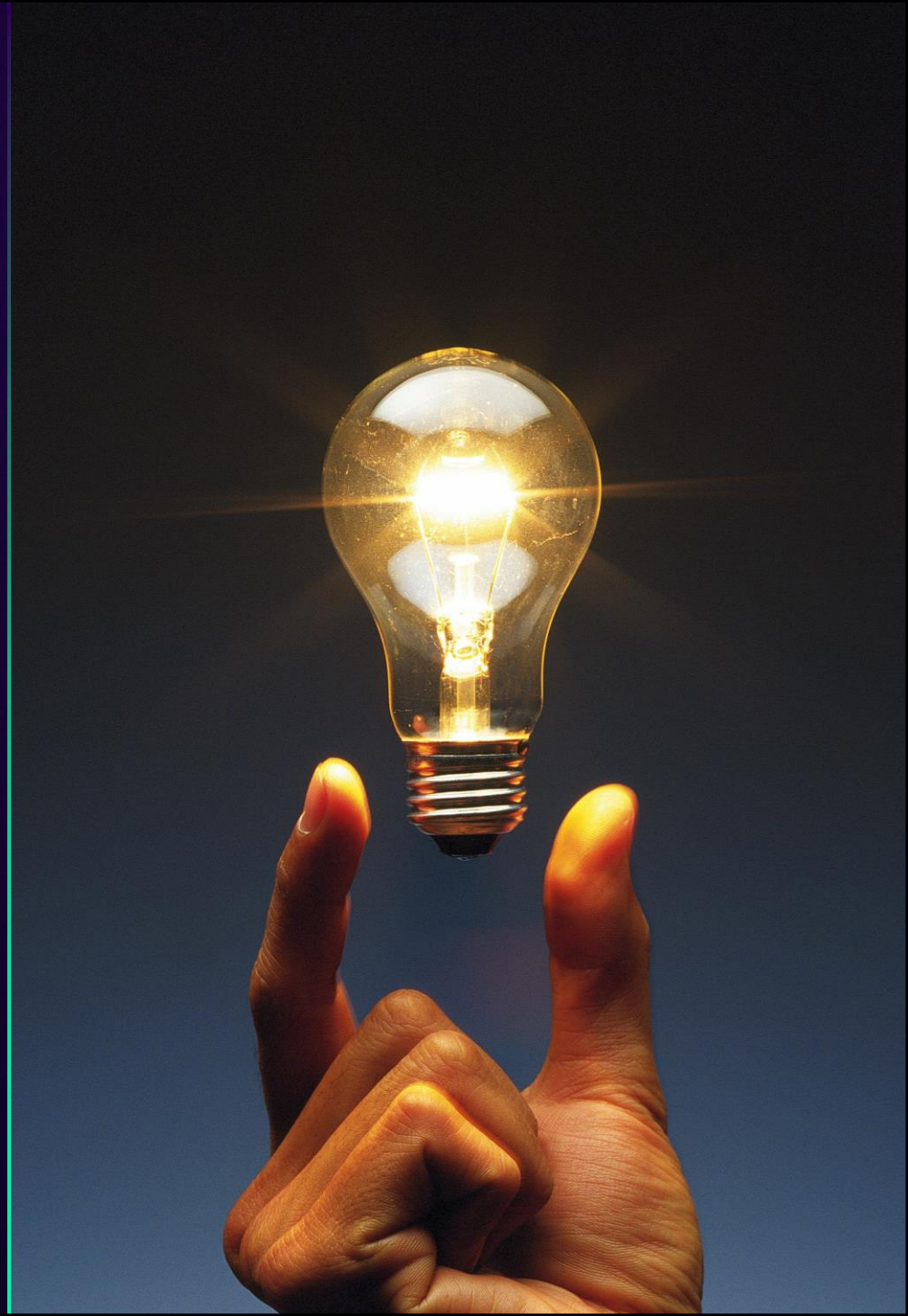
6 Leverage AWS integrations

7

8

9

10



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS Hybrid Nodes best practices

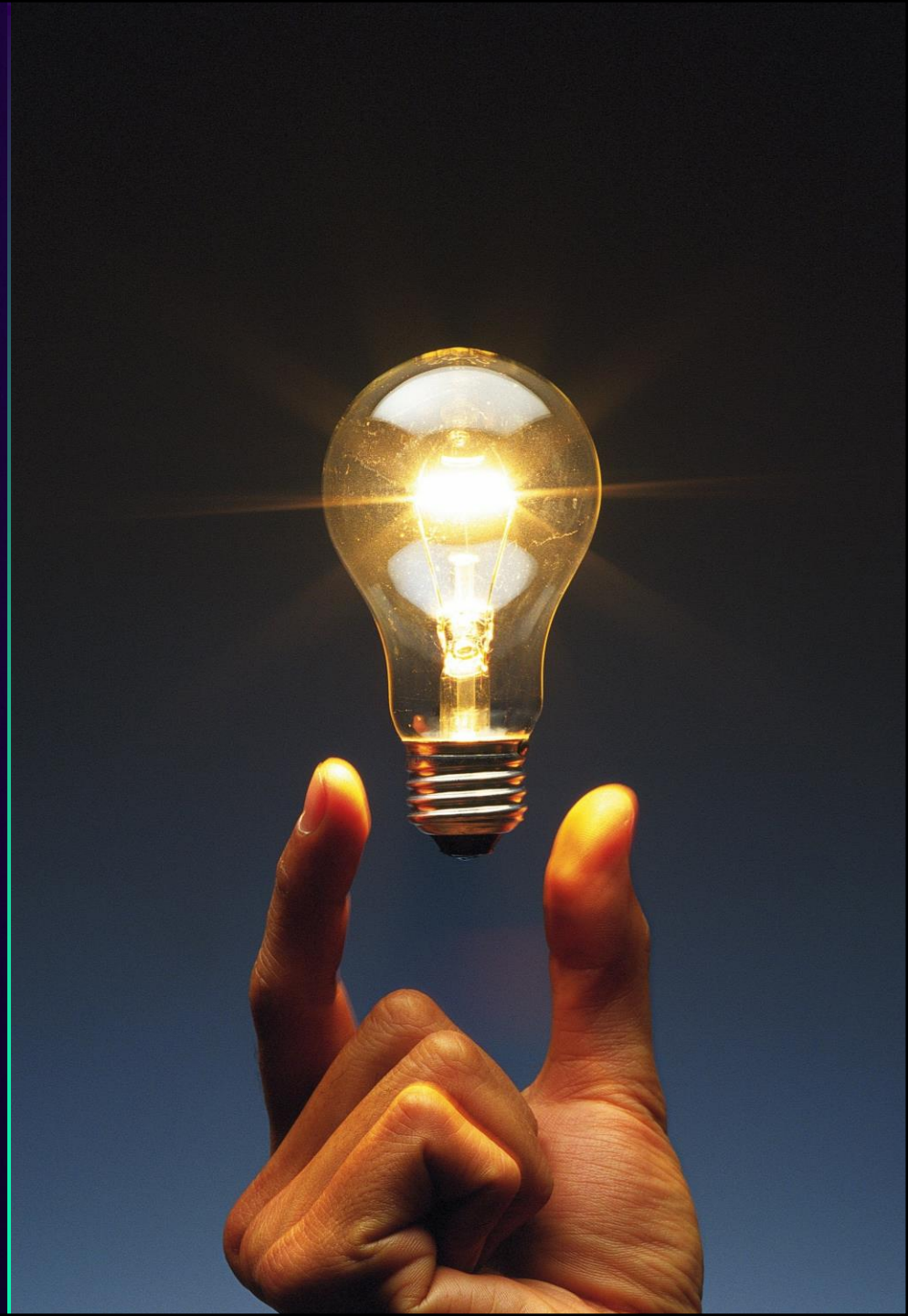
6 Leverage AWS integrations

7 Public **or** private API server endpoint access

8

9

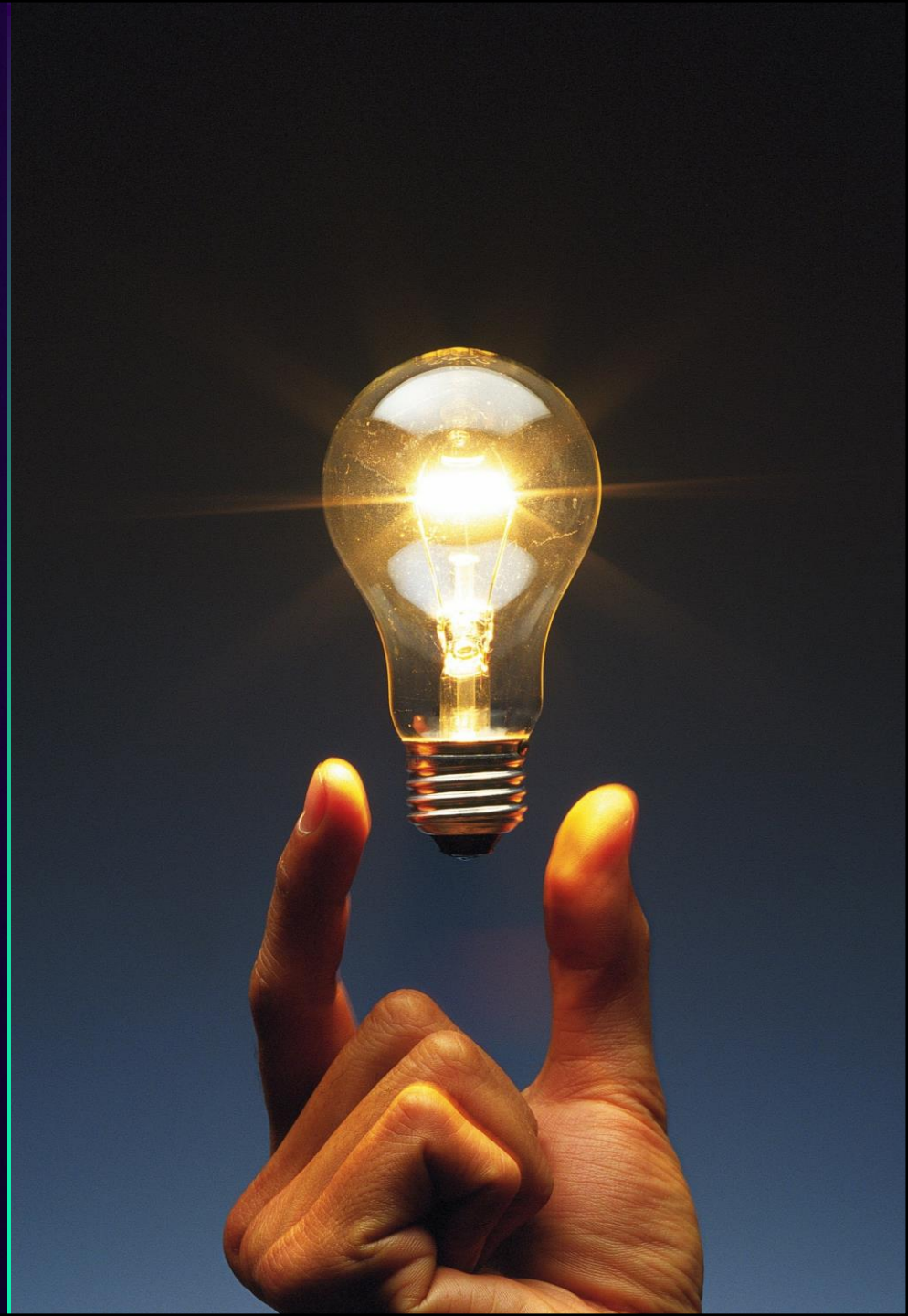
10



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS Hybrid Nodes best practices

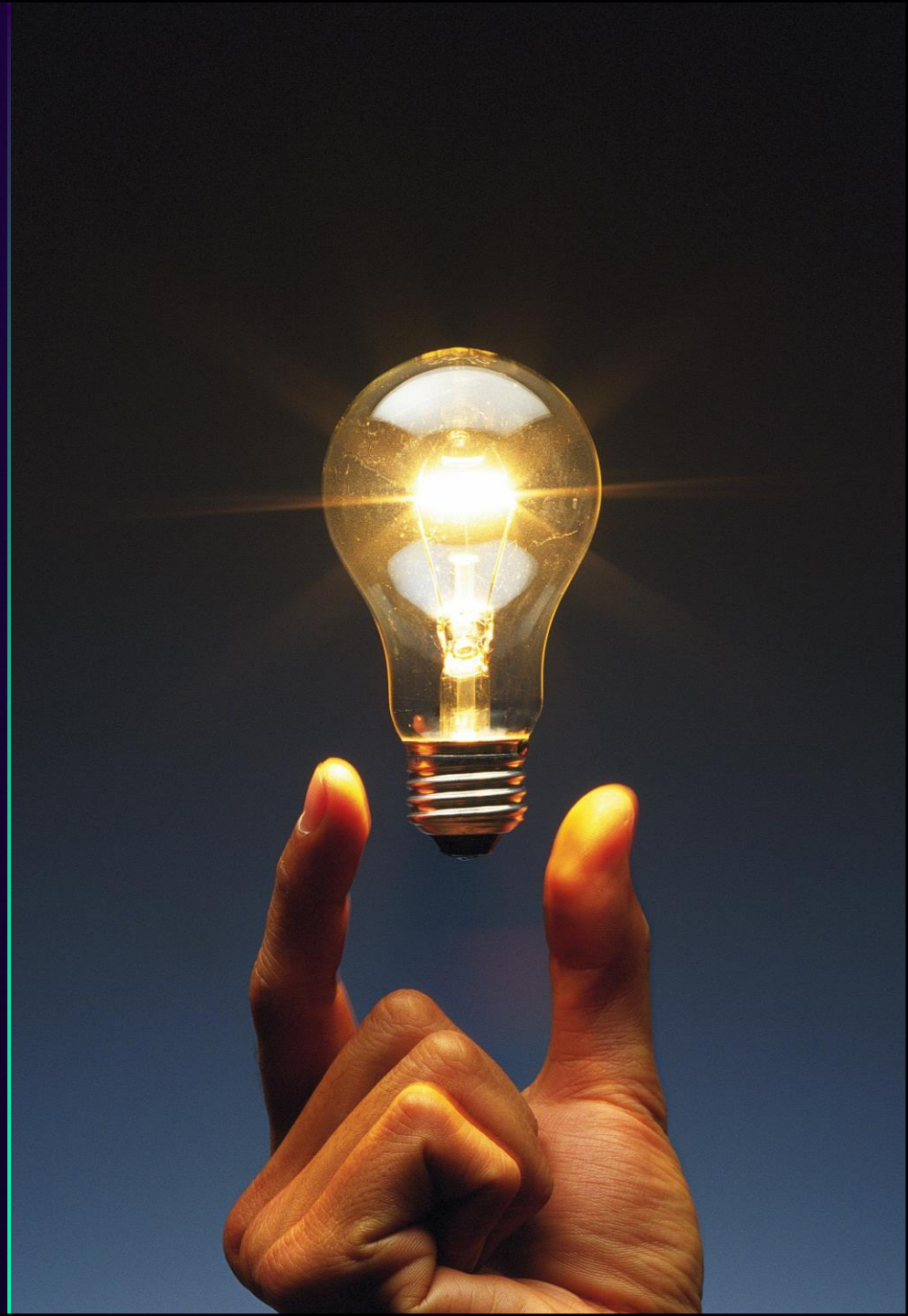
6. Leverage AWS integrations
7. Public **or** private API server endpoint access
8. Spread CoreDNS replicas
9. 
10. 



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS Hybrid Nodes best practices

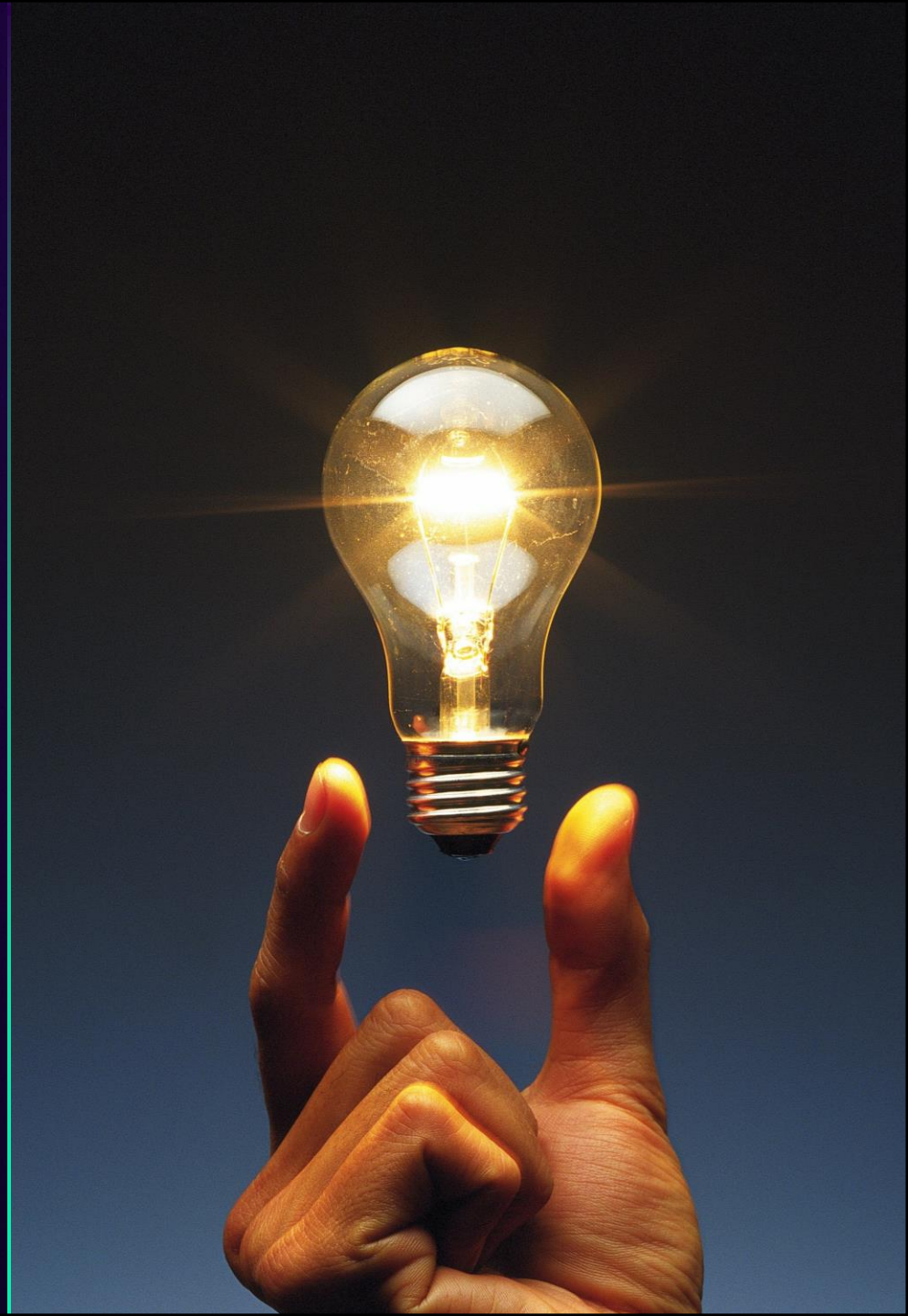
6. Leverage AWS integrations
7. Public **or** private API server endpoint access
8. Spread CoreDNS replicas
9. Tolerations and node labels
10.



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Amazon EKS Hybrid Nodes best practices

6. Leverage AWS integrations
7. Public **or** private API server endpoint access
8. Spread CoreDNS replicas
9. Tolerations and node labels
10. Rolling upgrades and delete unused nodes



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Northwestern Mutual use case

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

**For more than 165 years, Northwestern Mutual has been helping families and businesses achieve financial security**

Revenue $36 billion

FORTUNE 500 rank: 110

10,300+ financial professionals

8,200+ employees

Headquartered in Milwaukee, Wisconsin

Downtown NYC corporate office

Figures as of August 2024, unless otherwise noted

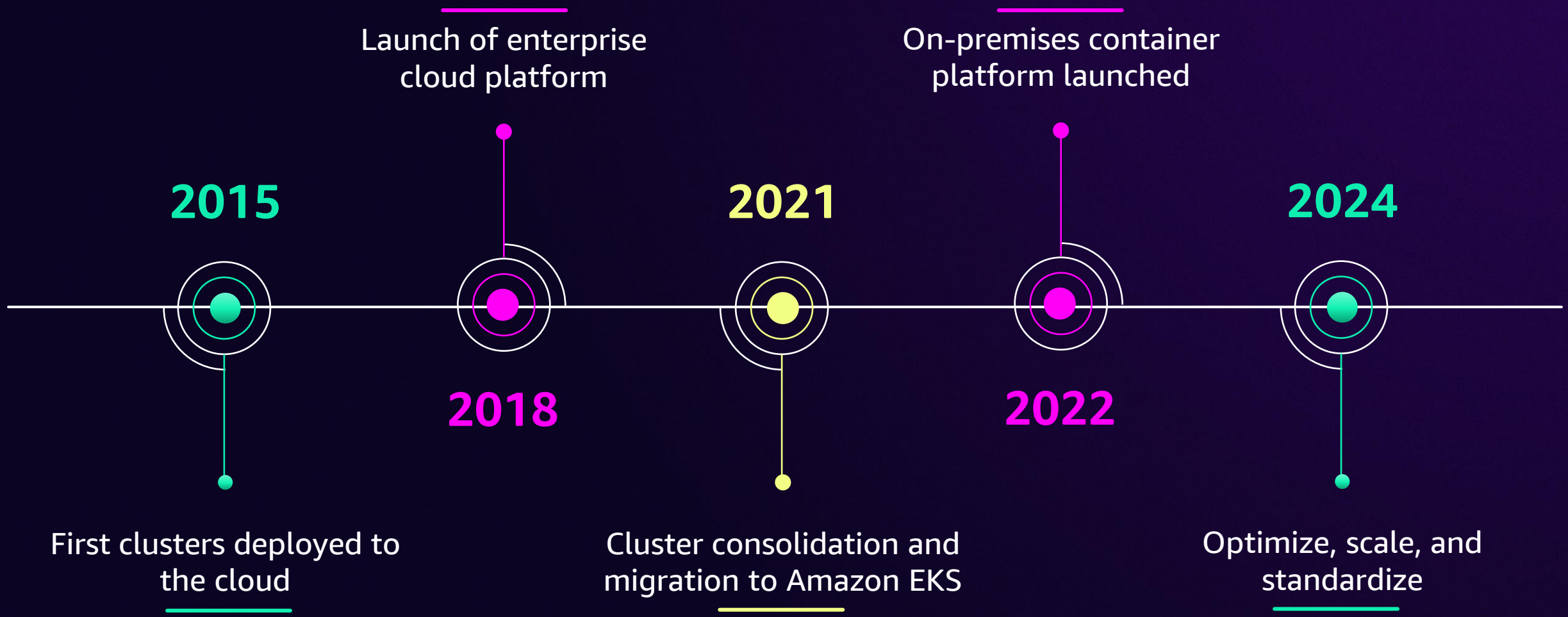
aws

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Northwestern Mutual®

# NM's Kubernetes journey

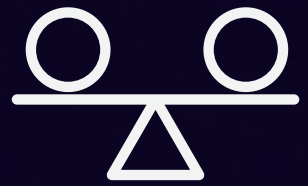
EVOLUTION OF COMPUTE MODERNIZATION




© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Northwestern Mutual

# NM’s cloud platform strategic themes



Stability

Security

Standardization

Simplification

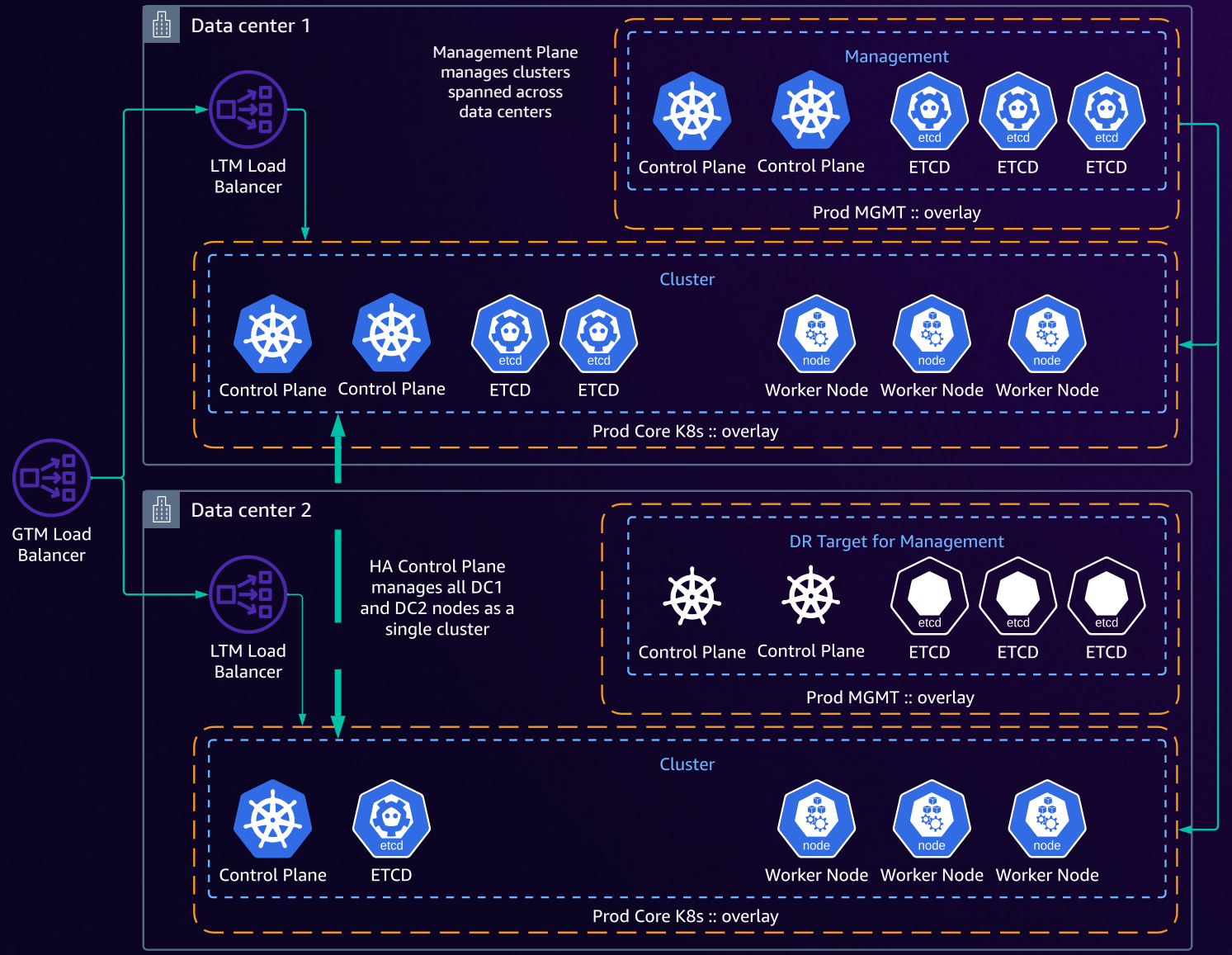
Spend

Staff

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

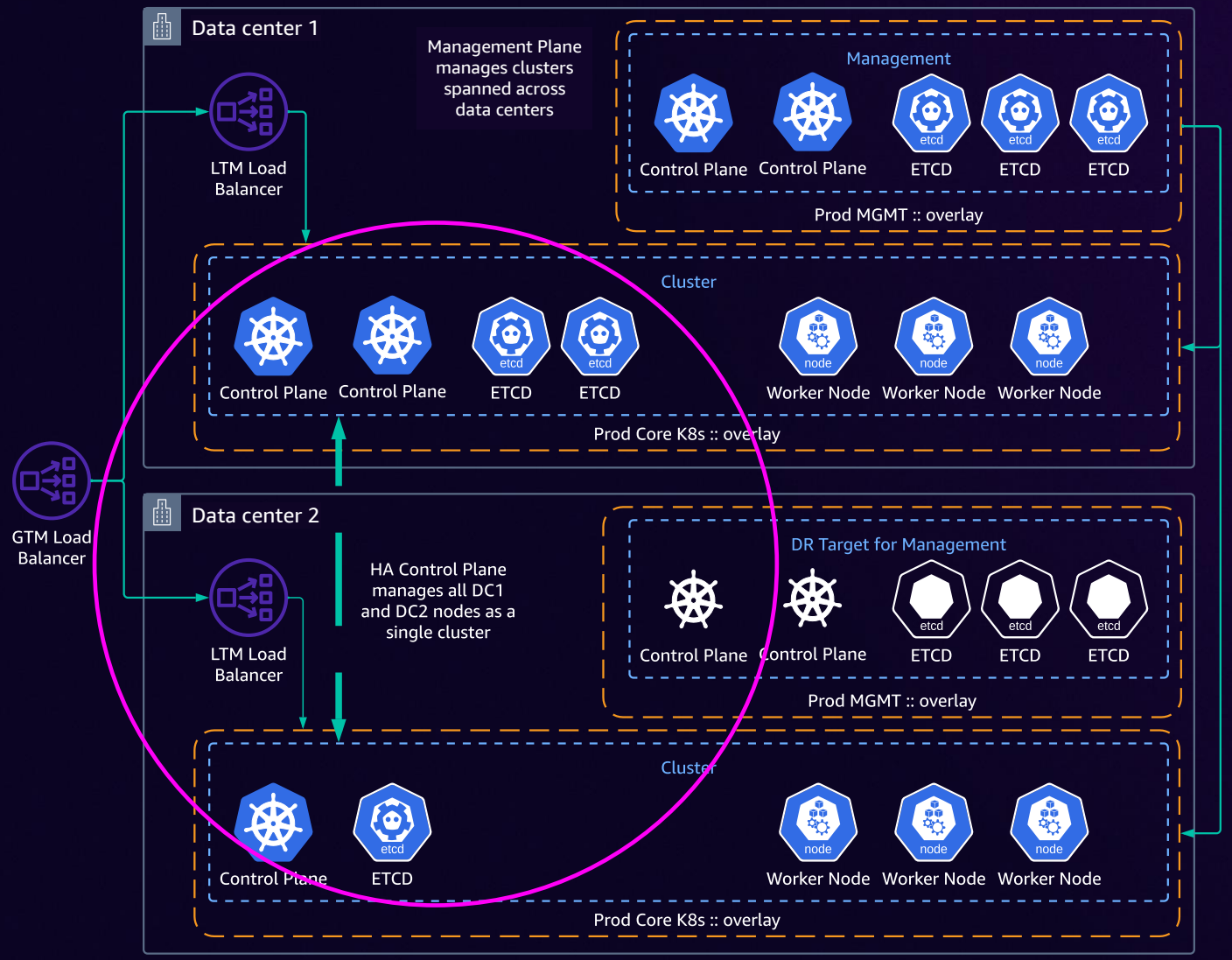
Northwestern Mutual

# Current state




© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# We have problems



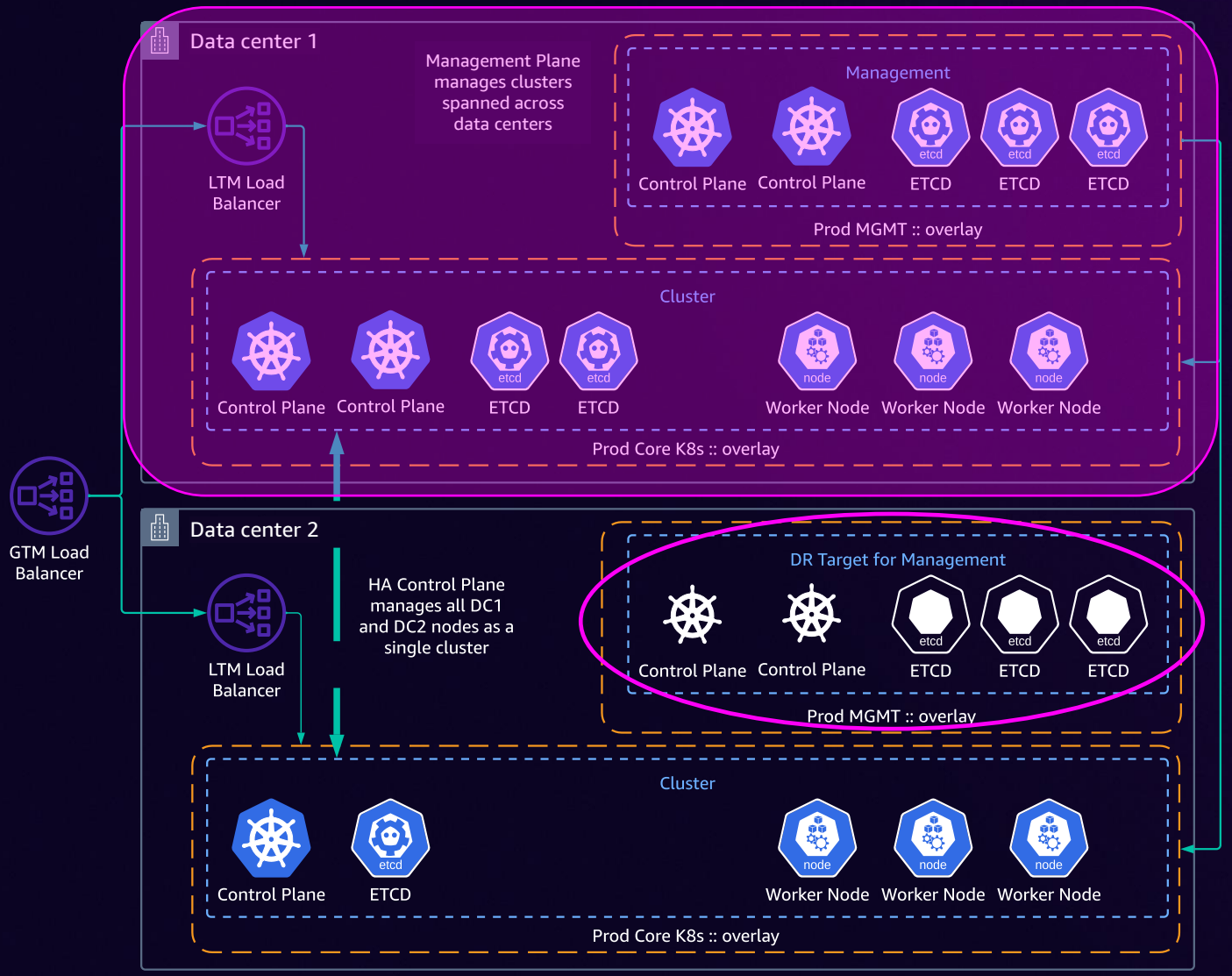

1

Loss of either data center results in loss of quorum

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Northwestern Mutual

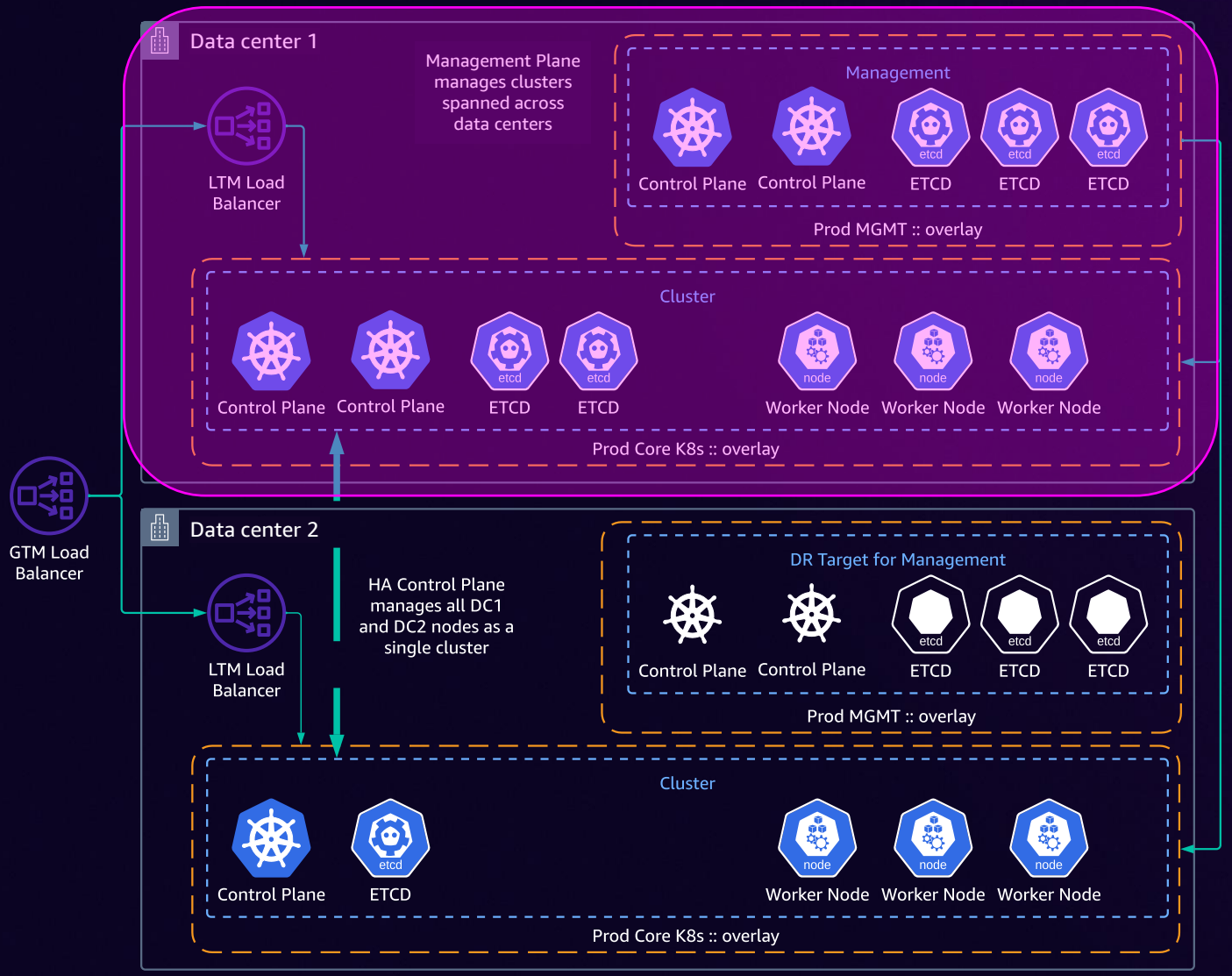
# We have problems




1. Loss of either data center results in loss of quorum
2. Loss of DC1 results in the loss of the management plane

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

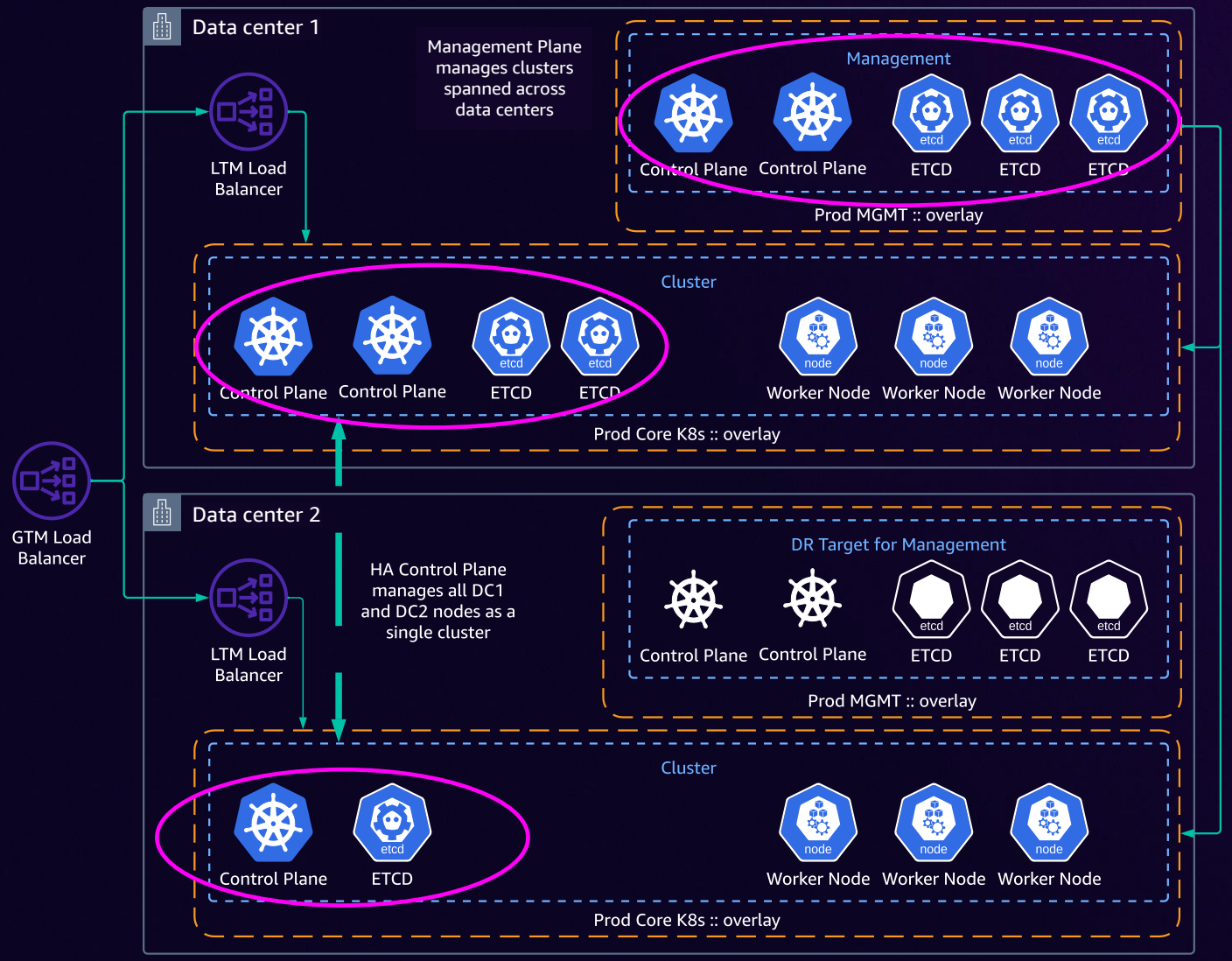
# We have problems




1. Loss of either data center results in loss of quorum
2. Loss of DC1 results in the loss of the management plane
3. Company decided to close primary data center facility

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# We have problems

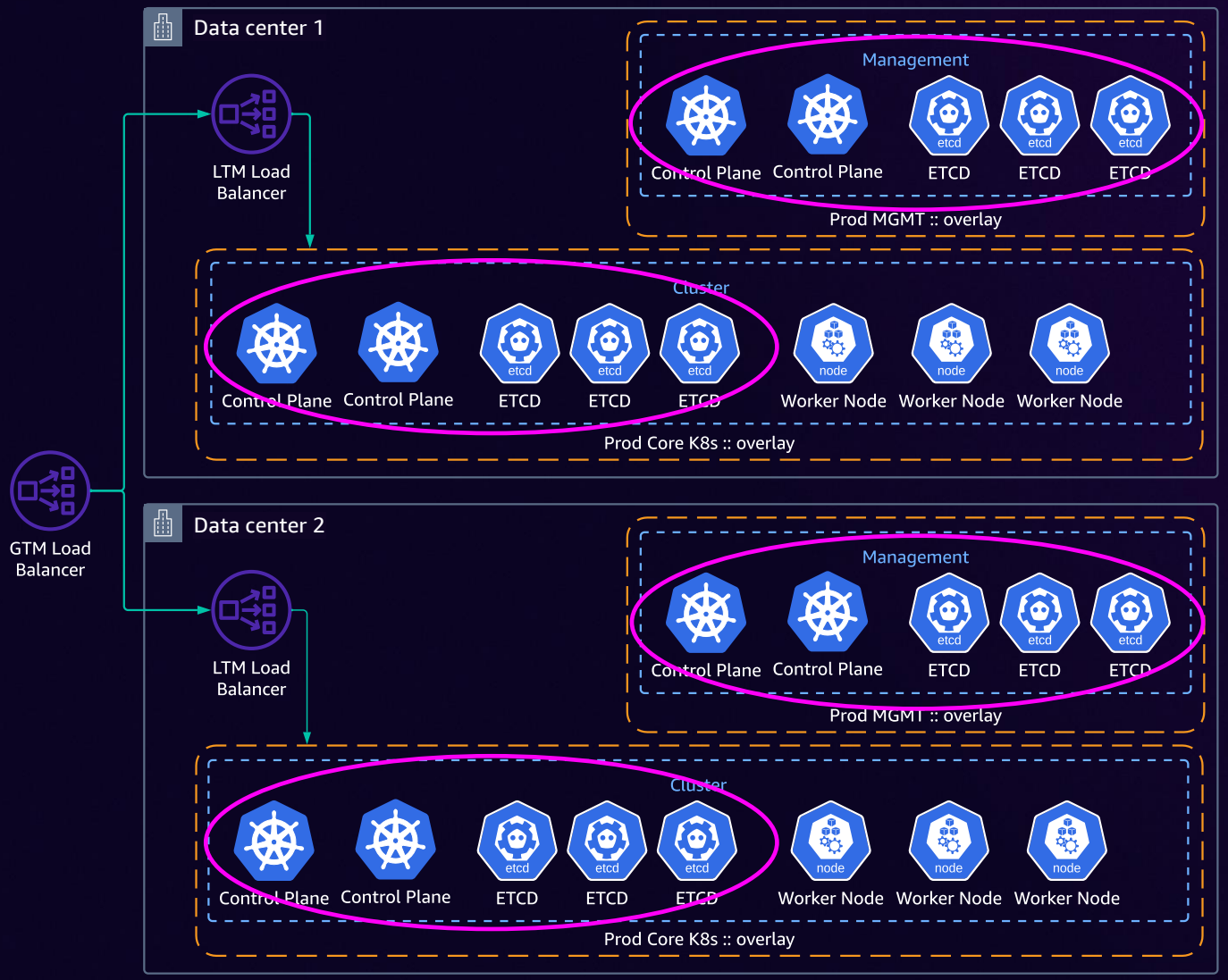



1. Loss of either data center results in loss of quorum
2. Loss of DC1 results in the loss of the management plane
3. Company decided to close primary data center facility
4. Effort needed to maintain platform is high

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Northwestern Mutual

# We have problems




1. Loss of either data center results in loss of quorum
2. Loss of DC1 results in the loss of the management plane
3. Company decided to close primary data center facility
4. Effort needed to maintain platform is high
5. Segmentation brings additional complexity and overhead

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# We need a better solution

OPTIONS WE CONSIDERED

01 Segment current platform

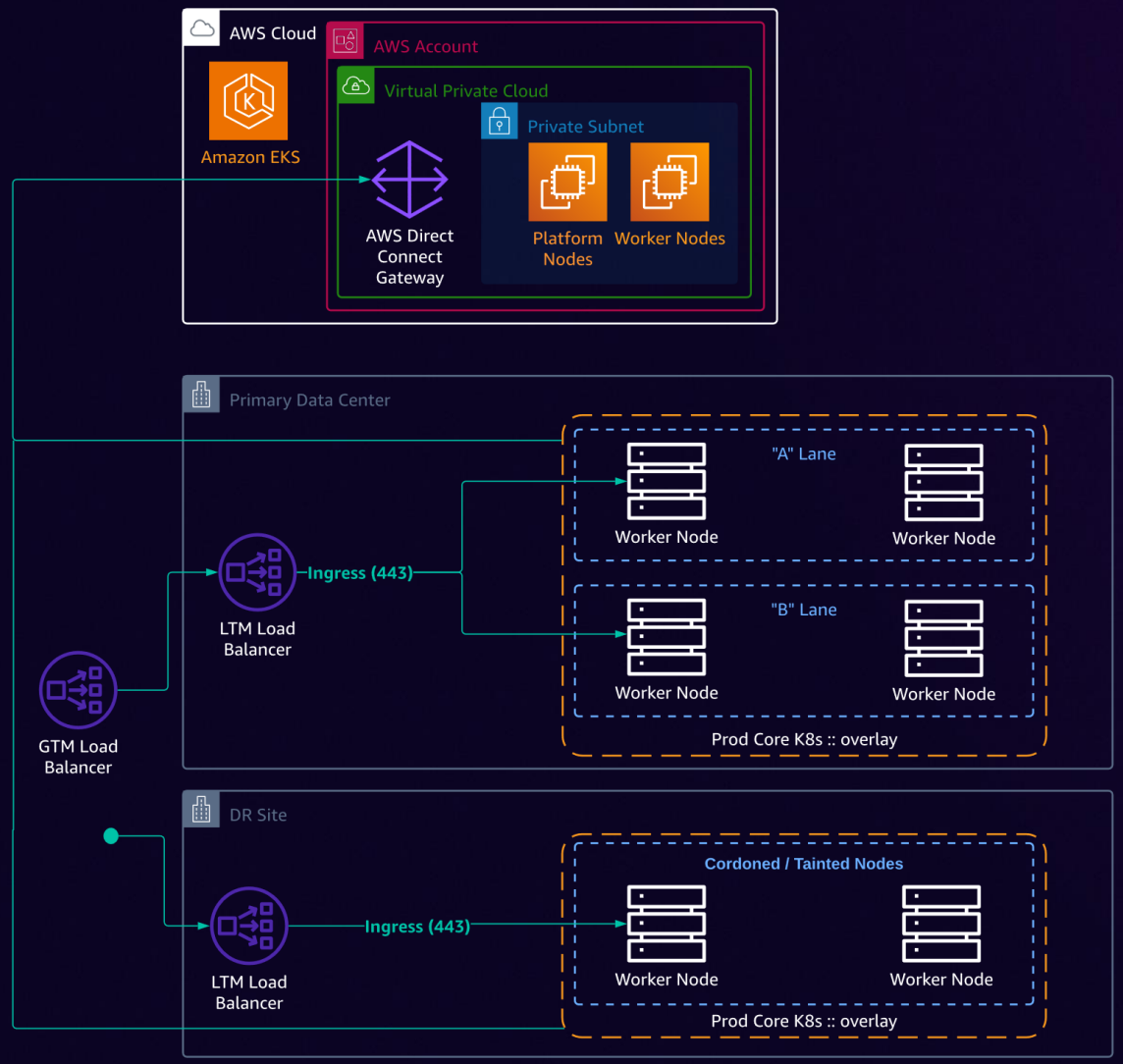
02 Retire the platform

03 Replace with EKS Anywhere

04 Build something custom

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# The best option – Amazon EKS Hybrid Nodes




1. Control plane resiliency is offloaded to AWS
2. Control plane maintenance is offloaded to AWS
3. Primary data center HA
4. Data center failover is as simple as changing node taints
5. Allows for transitional architecture patterns facilitating application modernization

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Northwestern Mutual

# Experience with Hybrid Nodes

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Northwestern Mutual

# Our Amazon EKS Hybrid Nodes configuration

## Network connectivity

AWS Site-to-Site VPN

AWS Direct Connect

## Infrastructure

Bare metal servers

Virtual machines

## Operating system

Ubuntu

Red Hat Enterprise Linux

Amazon Linux 2023

## Credential provider

AWS Systems Manager

AWS IAM Roles Anywhere

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

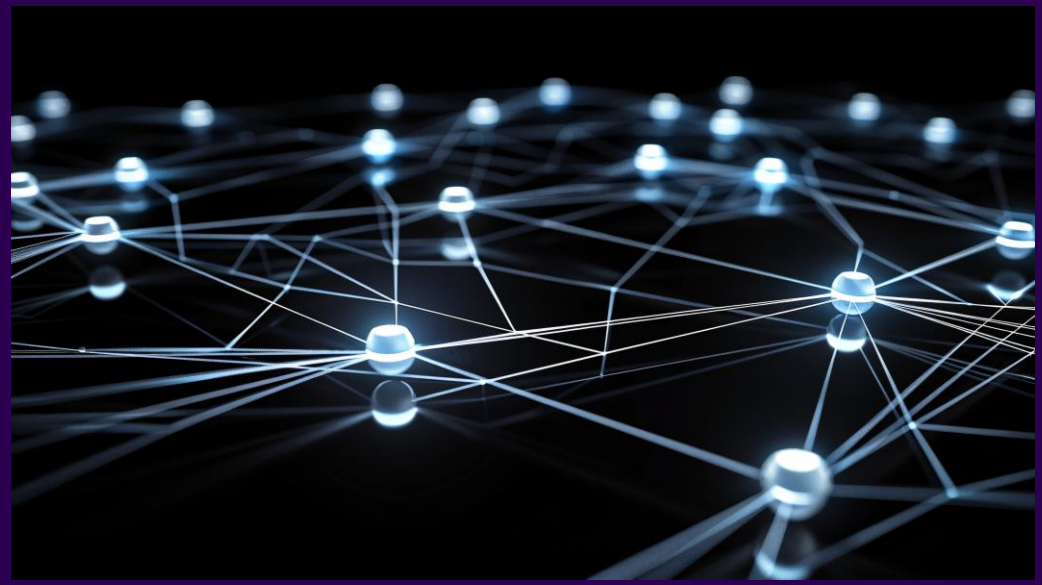
# Learnings

Bring networking and security teams along for the journey

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Learnings

Understand network flows of all your cluster components



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Learnings

**CHALLENGE:**

Security requirement that all node-to-node communication must be encrypted during transit

**SOLUTION:**

Enabling Cilium IPsec or Wireguard

aws

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Northwestern Mutual®

# Learnings

**CHALLENGE:**

Issues using IAM roles for service accounts (IRSA); errors while trying to assume roles

**SOLUTION:**

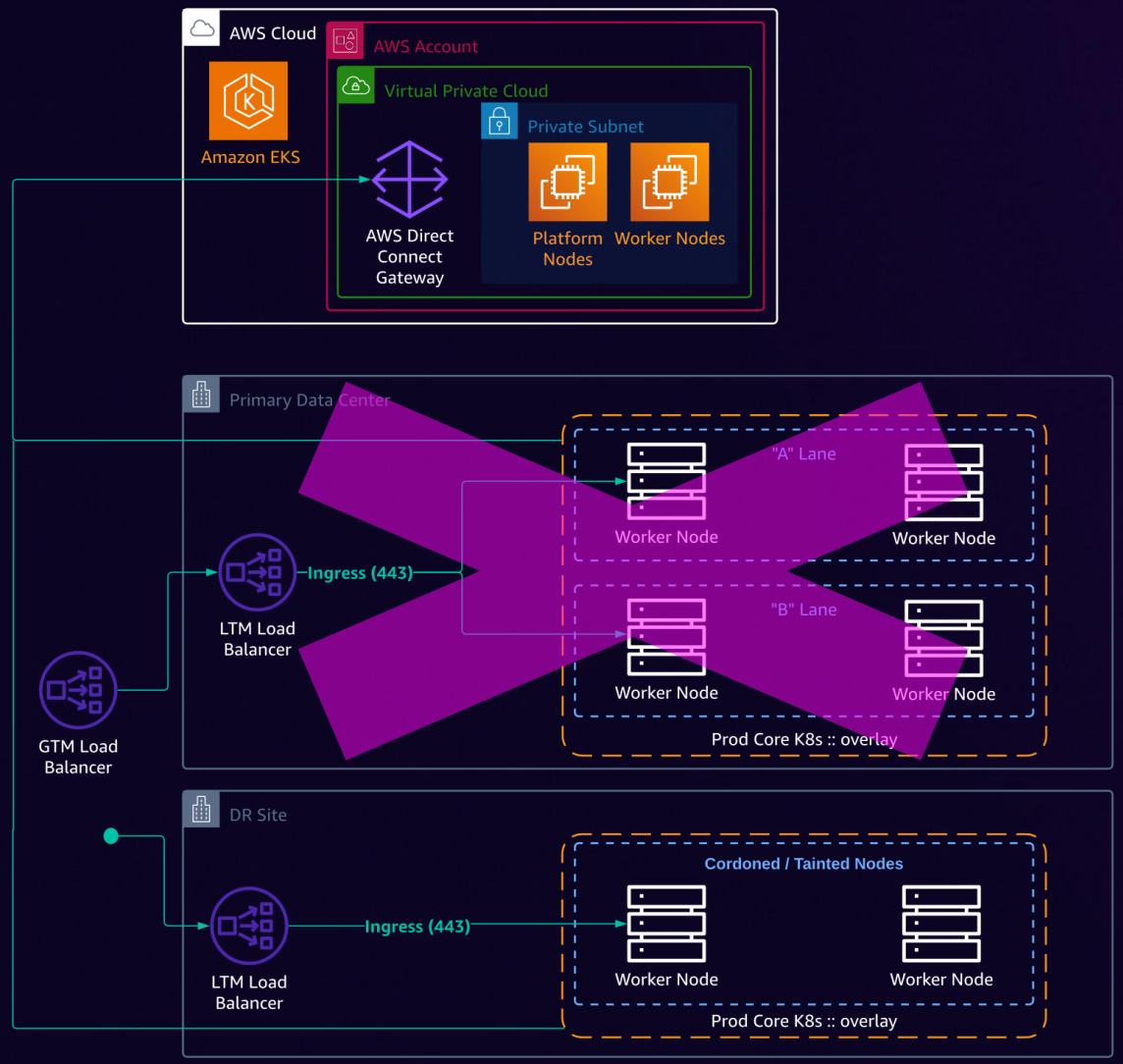
Ensure you set the Amazon EKS API server endpoints correctly for your allowed network configuration

aws

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Northwestern Mutual®

# Take our new design for a test drive



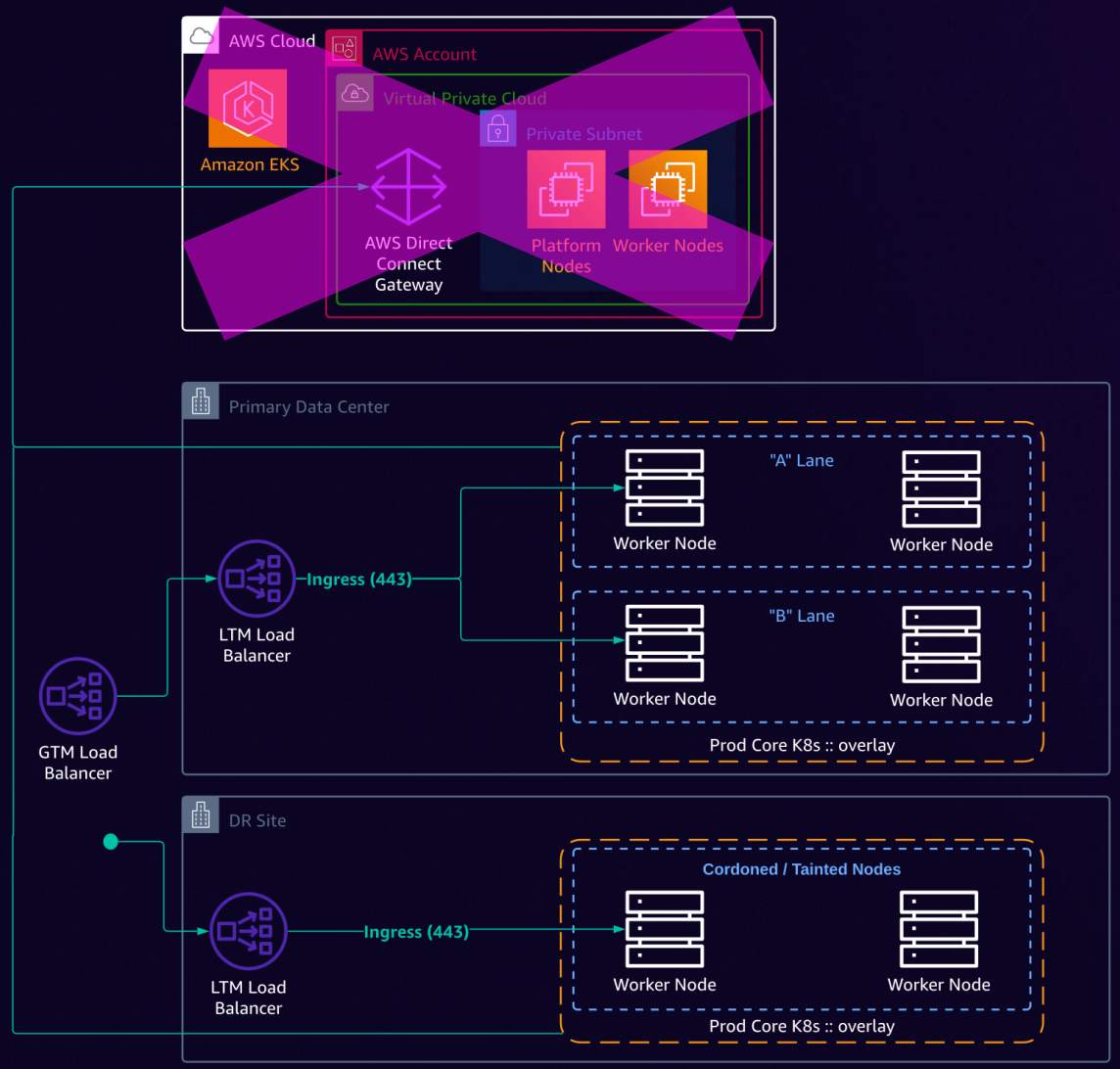

**Test case:**
DR scenario – loss of primary data center

**Results:**
- Worked exactly as expected, full recovery to DR site
- Recovery time < 20 min

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Northwestern Mutual

# Let’s see if we can really break it

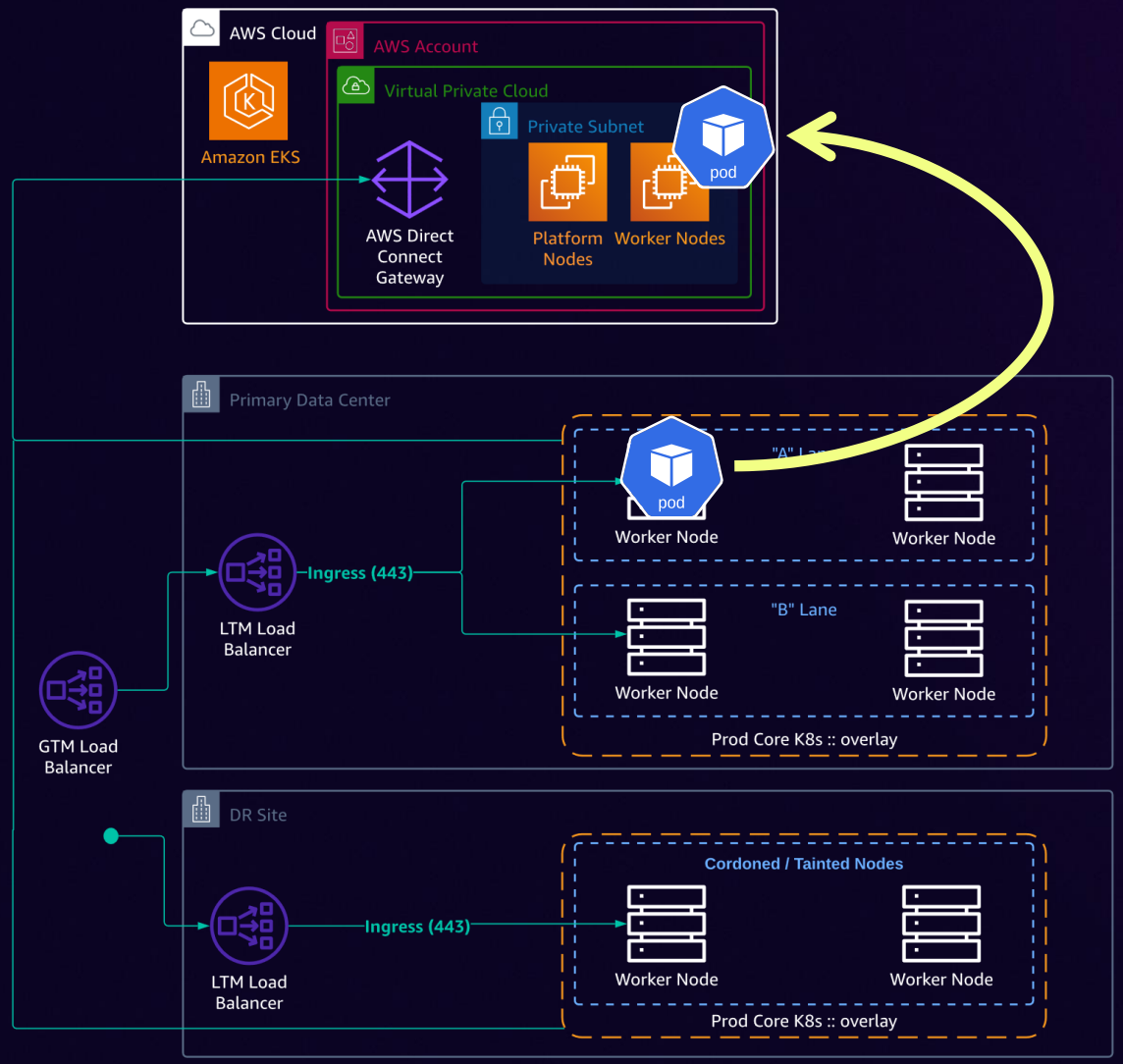



**Test case:**
Loss of connectivity to AWS or AWS Regional outage

**Results:**
- No disruption to workloads
- Recovery time = 0 min
- ** Workloads on Hybrid Nodes in a static state

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Let’s move things around




**Test case:**
Workload portability

**Results:**

- Moved according to Pod disruption budget and rollout strategy
- ** Works depending on workload dependencies and ingress routing

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Northwestern Mutual

Ease of joining the Hybrid Nodes required a lot **less custom** configuration than I would have expected.

**Russ Engel**

Lead Enterprise Architect, Northwestern Mutual

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The integration with SSM and IAM to connect nodes to AWS resources made it **super easy** to leverage on-prem compute for hybrid workloads.

**Anthony Carrasco**

Lead Cloud Platform Engineer, Northwestern Mutual

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Northwestern Mutual

# Benefits of using Amazon EKS Hybrid Nodes


Increases the **stability** and **resiliency** of our on-premises container platforms, easily reducing our recovery times


Maintains **consistent** security configuration and platform **guardrails**

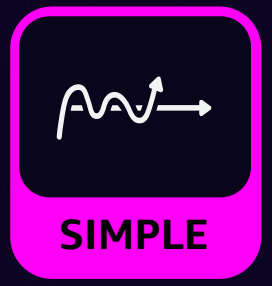

Allows for a **common** set of tooling, management processes, and developer **experience**

aws

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Northwestern Mutual®

# Benefits of using Amazon EKS Hybrid Nodes




Enables application modernization through an easier path to the cloud, while **eliminating** duplicate platforms and **complexity**


**Control** spend with a consumption-based cost model and **fully utilize** on-premises compute for workloads by hosting the control plane elsewhere


Allows more engineers to gain **experience** with cloud technologies and cloud-native way of working; increases **fungibility** of engineering workforce

aws

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Northwestern Mutual®

# Looking ahead

Amazon EKS Hybrid Nodes will support our data center migration efforts in the coming year

Plan for full production rollout by Q3 2025

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Northwestern Mutual

# Check out these other sessions

## KUB402-R, -R1: Amazon EKS: Infrastructure as code, GitOps, or CI/CD

Monday (Dec. 2) @ 4:30 PM – Caesars Forum, Summit 221
Wednesday (Dec. 4) @ 1:00 PM – MGM, 304

## KUB310: Amazon EKS for Edge and Hybrid Use Cases

Wednesday (Dec. 4) @ 10:00 AM - Wynn, Level 1 Lafite 4

## KUB312: Automated cluster infrastructure with Amazon EKS and Karpenter

Wednesday (Dec. 3) @ 2:30 PM – MGM, Chairmans 355

## KUB201: The future of Kubernetes on AWS

Thursday (Dec. 5) @ 11:30 AM – MGM, Grand 122

aws
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Continue your Amazon EKS learning

## Learn at your own pace

Take the **Amazon EKS Workshop** to expand your EKS skills

## Increase your knowledge

Use our **Best Practices Guide** to build your Kubernetes knowledge

## Earn Amazon EKS badge


Demonstrate your knowledge by achieving **digital badges**

https://github.com/aws-samples/reinvent24

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Thank you!

Please complete the session survey in the mobile app

**Chris Splinter**
LinkedIn: csplinter

**Jon Ogden**
LinkedIn: jontogden

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.