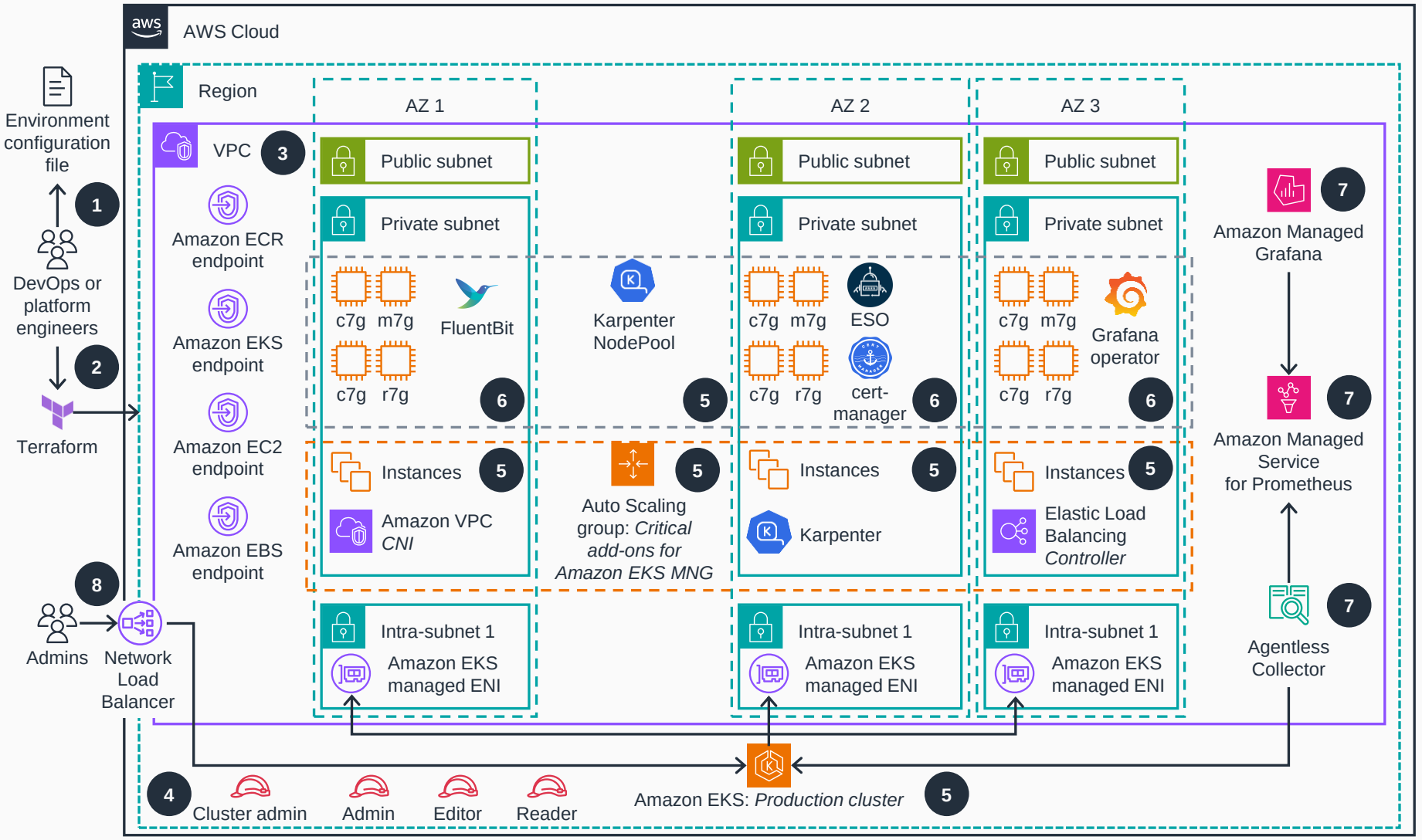
Guidance for Automated Provisioning of Application-Ready Amazon EKS Clusters

This architecture diagram shows how to provision an Amazon Elastic Kubernetes Service (Amazon EKS) cluster with a production-ready configuration and critical add-ons in a single AWS account environment. This slide details steps 1–6; steps 7-8 are detailed on the next slide.



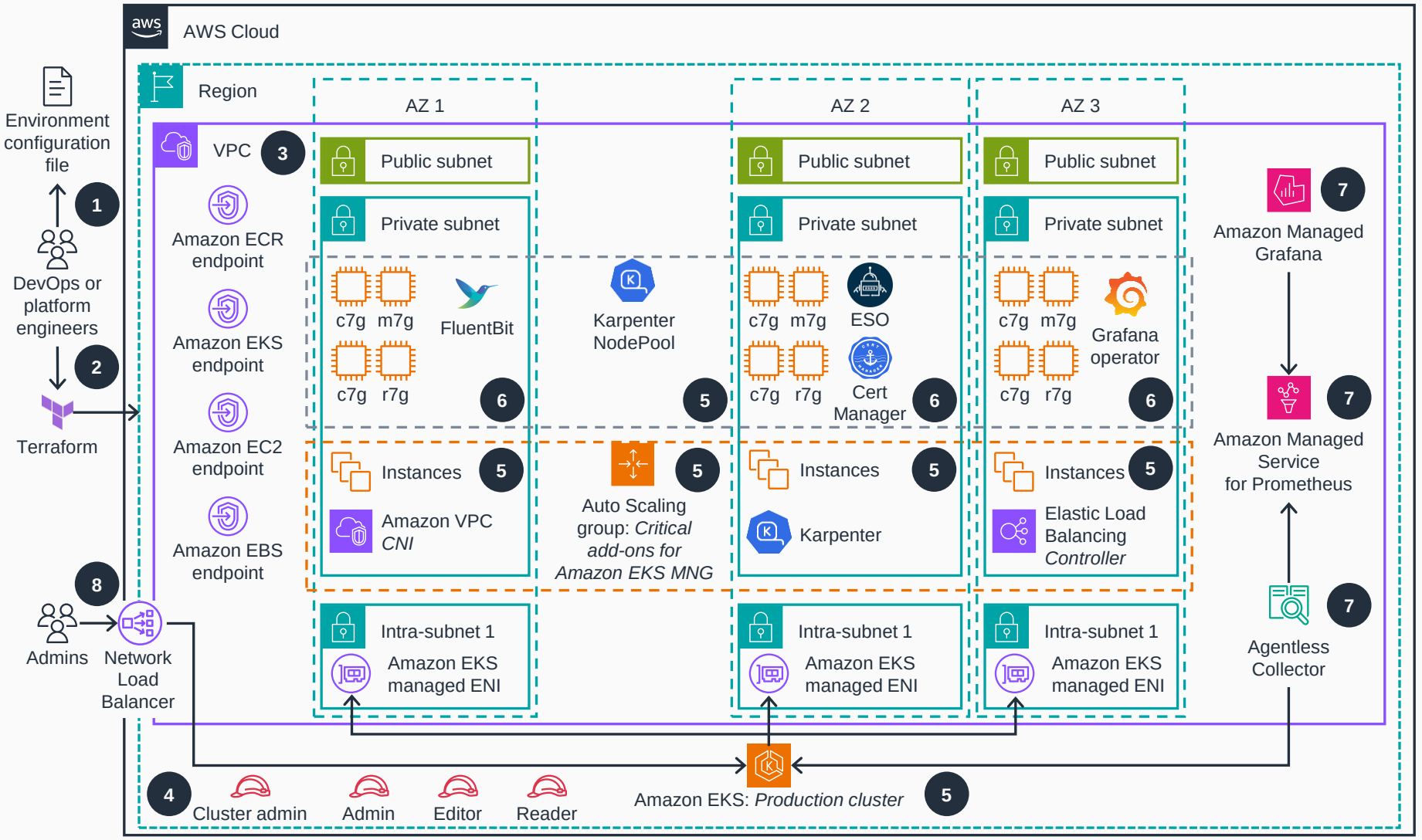
1. Define a per-environment Terraform variable file that controls all environment-specific configurations. This configuration file is used in all steps of the deployment process by all infrastructure as code (IaC) configurations to create different **Amazon Elastic Kubernetes Service (Amazon EKS)** environments.
2. Apply the environment configuration using Terraform.
3. An **Amazon Virtual Private Cloud (Amazon VPC)** is provisioned based on the specified configuration. According to best practices for reliability, three Availability Zones (AZs) are configured with corresponding virtual private cloud (VPC) endpoints to provide access to resources deployed in your VPC. These resources might include **Amazon Elastic Container Registry (Amazon ECR)**, **Amazon EKS**, **Amazon Elastic Compute Cloud (Amazon EC2)**, and **Amazon Elastic Block Store (Amazon EBS)**.
4. User-facing **AWS Identity and Access Management (IAM)** roles (cluster admin, admin, editor, and reader) are created for various access levels to **Amazon EKS** cluster resources, as recommended in Kubernetes security best practices.
5. The **Amazon EKS** cluster is provisioned with a managed nodes group (MNG) that runs critical cluster add-ons (such as CoreDNS, Karpenter, and AWS Load Balancer Controller through **Elastic Load Balancing**) on its compute node instances. Karpenter will manage the compute capacity to other add-ons (as well as business applications that your users deploy) while prioritizing instances powered by **AWS Graviton processors** for better price performance. **Amazon EKS** managed elastic network interfaces (ENIs) are deployed in isolated subnets.
6. Other relevant **Amazon EKS** add-ons (such as cert-manager or External Secrets Operator (ESO)) are deployed based on their configurations defined in the corresponding Terraform configuration files (step 1).

Reviewed for technical accuracy October 8, 2024

AWS Reference Architecture

Guidance for Automated Provisioning of Application-Ready Amazon EKS Clusters

Steps 7–8



7 An AWS managed observability stack is deployed (if configured), including **Amazon Managed Service for Prometheus** (with an AWS managed collector for **Amazon EKS**) and **Amazon Managed Grafana**. In addition, a Grafana operator add-on is deployed with a set of predefined Grafana dashboards to get you started.

8 One or more **Amazon EKS** clusters with important add-ons (optionally configured with a managed observability stack and **IAM** role-based access control) are available for your production workload deployment. These clusters' Kubernetes APIs are exposed using Network Load Balancers.

Reviewed for technical accuracy October 8, 2024

AWS Reference Architecture