NII - Containers

Topics

「管理基盤」on EKS

- t3.xlarge x 5
    - 4x pods

1. CI/CD

TODO: 喋ったことを追記する

- Teams
    - Who deploys?
    - Who operates apps?
    - Who operates K8s clusters?
- Automation
    -
- Operation
    -

2. 管理運用

- Upgrades
    - Control plane - one click upgrade on EKS
        - EKS
            - NLB
            - at least 2 API servers
            - at least 3 etcd nodes
    - Data plane - Kubernetes supports 2 version-diff between control-plane(e.g. 1.13) and data-plane(e.g. 1.11 <)
        - Node it self
        - System components
            - on-prem
                - use Ansible, etc.
                - Setup Worker Nodes
                    - use those to upgrade
            - on-cloud
                - Add new worker nodes with the new AMI
                - Drain old nodes
                    - Pre-installed (Optimized AMI)
                        - kubelet

            - [CON] CoreDNS - kube-system
            - [CON]VPC CNI plugin - kube-system
        - User installed
            - ALB Ingress Controller
            - Metrics Server
            - HPA
            - Cluster Autoscaler / Escalator
                - based on Kubernetes events
                - Pod Priority
            - CloudWatch Alarm + ASG
                - CPU/Memory Usage or Reservation
            - Log collector
                - logrotate
                - cloudwatch-agent
                - fluentd-agent
            - Helm
            - etc., etc.
- Designing cluster separation
    - Namespaces
        - Resource quota
    - Blast radius
        -

3. セキュリティ

- Clusters
    - Keep API server secure
        - External
            - DON'T expose
        - Internal
            - Role-Based Access Control
                - ~~ALL system:master~~
            - Pod Security Policy (k8s 1.13 ~)
                - x privileged
                - nonRootUser
- Node
    - Session Manager instead of SSH
        - IAM auth instead of SSH key
    - DO NOT Install daemons or anything directly
        - Deploy them as daemonset via Container orchestrator
- Services/Deployments
    - East-west traffic

        - Security Group
        - AuthN/AuthZ
    - to AWS services
        - IAM
- Containers
    - Runtime
        - 3rd-party SaaS
            - Aqua
            - Twistlock
            - (Trend Micro)
    - Image
        - Scanning
            - 3rd-party SaaS
                - Aqua
                - Twistlock
            - OSS
                - Clair (by CoreOS) - AWS Blog
                - Vuls (by FutureArchitect)
        - Signing
            -
- Apps
    - 3rd-party
        - Snyk

4. 鍵管理

鍵？
KMS
CloudHSM

5. ログの話

分散トレーシング
AWS X-Ray (サービスとそこと通信をするための App SDK)

- X-AMZ-TRACE-ID ...?

突き進めていくとサービスメッシュ (App Mesh)

- プロキシ使うー便利ー