ADCONF

拨云见日
万壑归流

云原生安全攻防启示录

李帅臻-网星安全 御守实验室负责人

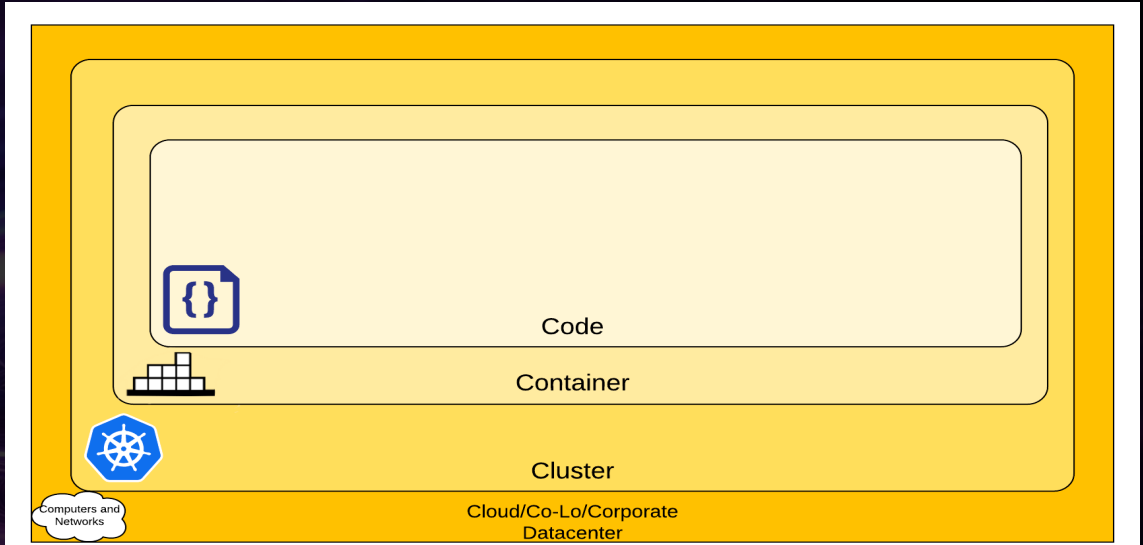
contents|目录

CONTENTS

/01

4C' 云原生安全

4C' 云原生安全

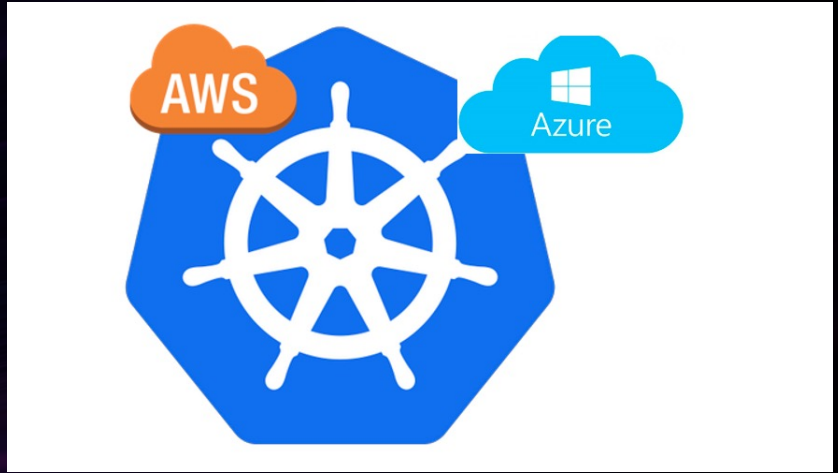

Code
Container
Cluster
Computers and Networks
Cloud/Co-Lo/Corporate Datacenter

4C' 云原生安全 - Cloud

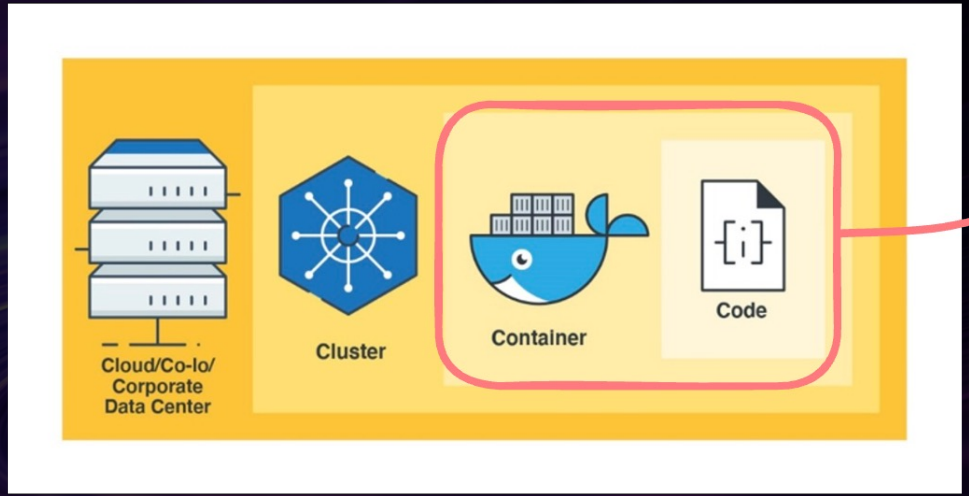
- ✓ 身份和访问管理漏洞
- ✓ API滥用和未经授权访问
- ✓ 云产品信任关系滥用
- ✓ API密钥泄露
- ✓ 云平台元数据滥用
- ✓ 身份冒用

4C' 云原生安全 - Cluster

- ✓ 多租户隔离漏洞
- ✓ Secrets对象滥用
- ✓ 服务间未授权访问
- ✓ APIServer未授权访问
- ✓ K8s自身漏洞
- ✓ 错误配置



4C' 云原生安全 – Container & Code



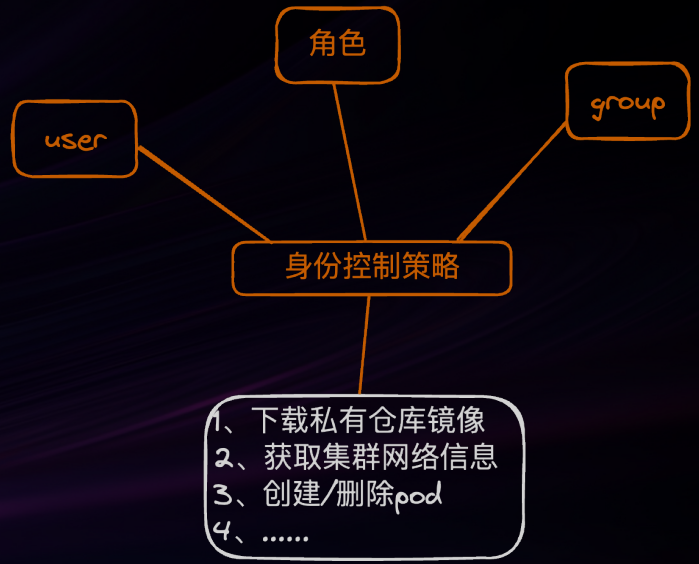
- ✓ 镜像漏洞
- ✓ 容器逃逸
- ✓ 内核漏洞
- ✓ 错误配置
- ✓ 应用程序漏洞

/02

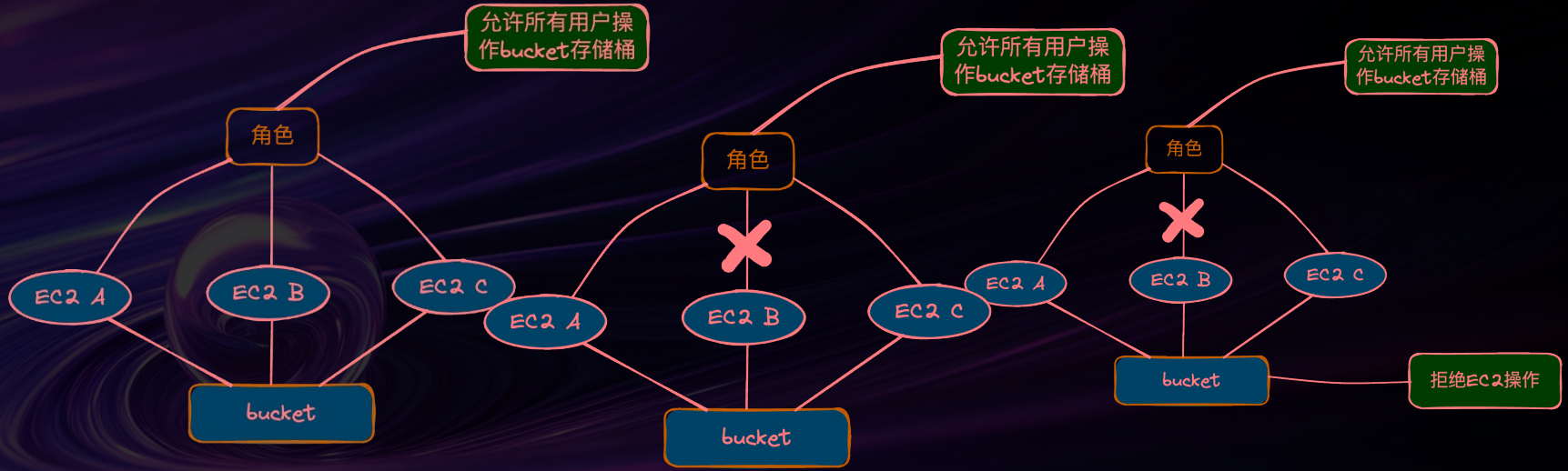
云上身份攻击

4C' 云原生安全 – Container & Code

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::bucket",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp":
"192.168.1.6"    }
            }
        }
    ]
}
```

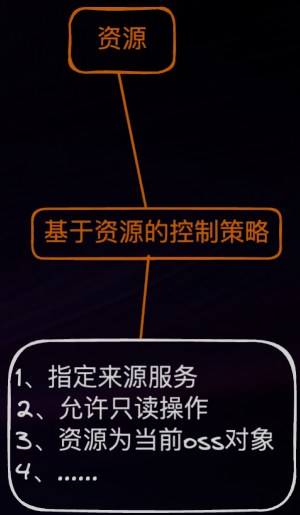


基于资源的策略


允许所有用户操作bucket存储桶
角色
EC2 A
EC2 B
EC2 C
bucket
允许所有用户操作bucket存储桶
角色
EC2 A
EC2 B
EC2 C
bucket
允许所有用户操作bucket存储桶
角色
EC2 A
EC2 B
EC2 C
bucket
拒绝EC2操作

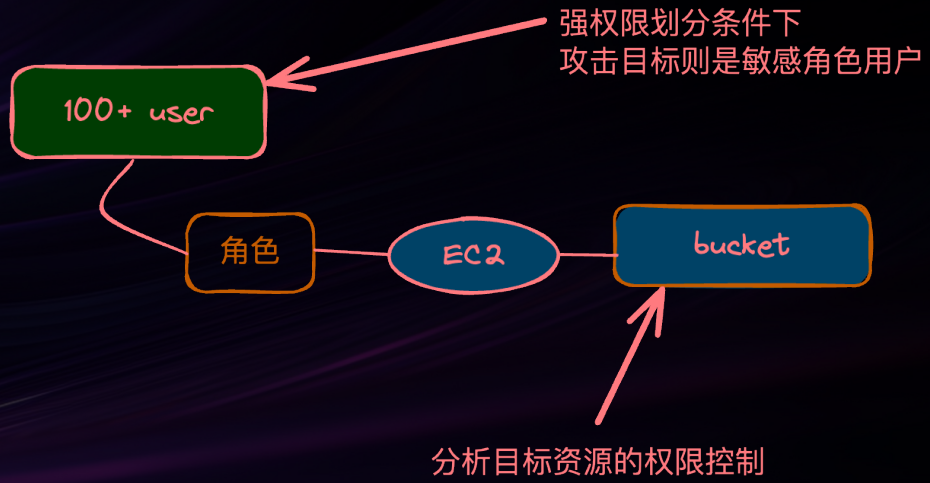
基于资源的策略

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AddCannedAcl",
      "Effect":"Allow",
      "Principal": {"AWS": ["arn:aws:iam::798436:root"]},
      "Action":["s3:PutObject"],
      "Resource":"arn:aws:s3:::bucket/*",
      "Condition":{"StringEquals":{"s3:x-amz-acl":["public-read"]}}
    }
  ]
}
```



基于资源的策略攻击思路

- ✓ 如果权限细化的非常严格，则敏感角色是我们有限攻击目标
- ✓ 权限过高则则将目标放在资源上
- ✓ 即使一个账户没有任何权限，依然可以对配置基于资源的策略对象进行操作

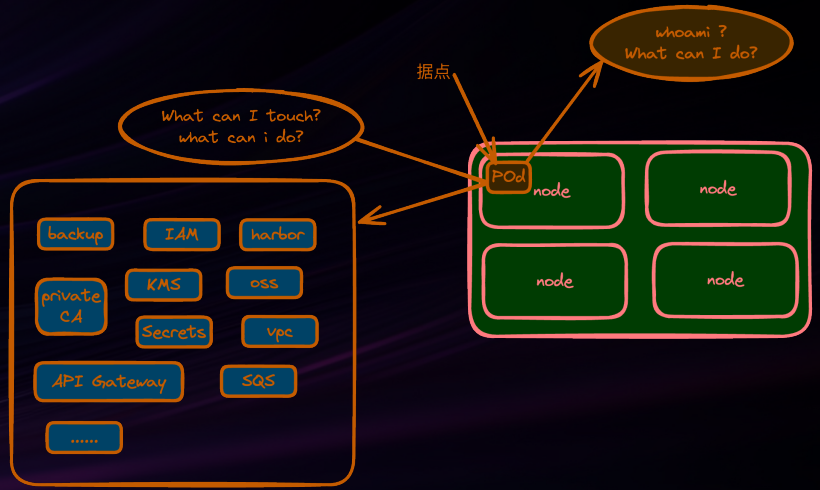


基于资源的策略攻击思路

当我们掌握一个身份后，我们非常关注它的身份策略，以及他可以执行的操作，同时我们应该注意环境中可能存在很多资源，**这些资源可能具备预置的某些权限信任关系**，这些可能是我们可以利用的一个突破口。

基于资源的策略攻击思路

- ✓ 基于资源的策略不仅仅应用在S3上，还有大量云上基础资源，任何一个受到攻击都会影响巨大

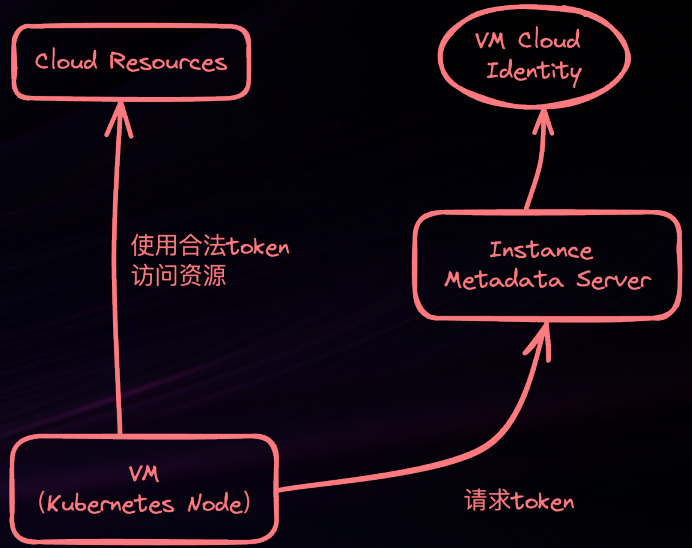


案例分析


Cloud - OSS
update:
EXE/Dll
Get
App
实时检查
checkTools
OSS
权限由gut变为get/put
C2 Server
制作木马

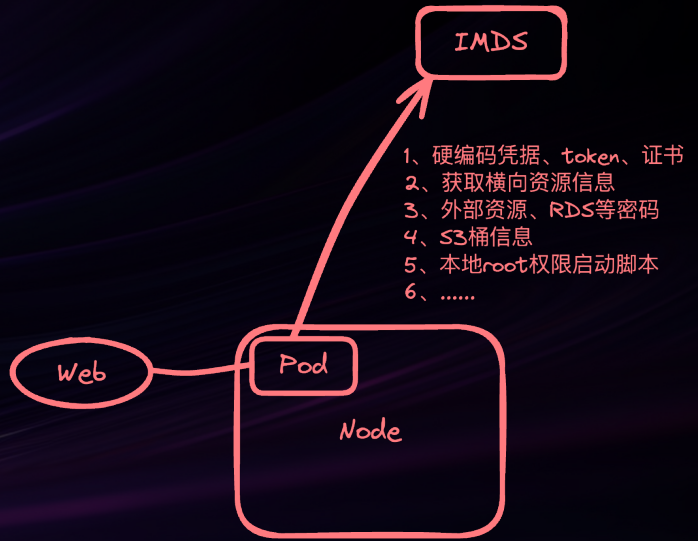
IMDS攻击利用

- ✓ Meta-data：用来查询服务器实例ID、网络ID等信息
- ✓ User-data：在第一次启动或重新启动服务器时安装软件、下载代理、下载配置文件、启动某些程序、检查配置等操作



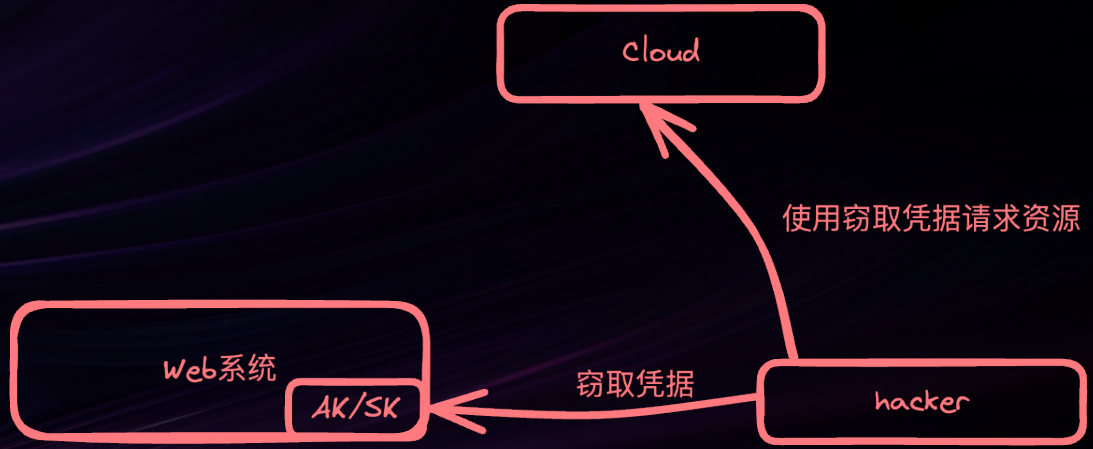
IMDS攻击利用

- ✓ 提权
- ✓ 敏感信息收集
- ✓ 横向移动
- ✓ 可以访问哪些资源
- ✓ 硬编码凭据
- ✓ 以root权限运行的脚本



AK/SK利用防护绕过

- ✓ 新启服务器实例
- ✓ 云函数
- ✓ VPC



/03

从K8s到Cloud

从K8s到Cloud

获取到一个pod之后，它的权限可能是这样的

```
AmazonEC2ContainerRegistryReadonly {
    "Effect":"Allow",
    "Action":[
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:DescribeImages",
        "ecr:BatchGetImage",
        "ecr:GetLifecyclePolicy",
        "ecr:GetLifecyclePolicyPreview",
        "ecr:ListTagsForResource",
        "ecr:DescribeImageScanFindings"
    ],
    "Resource":"*"
}
```

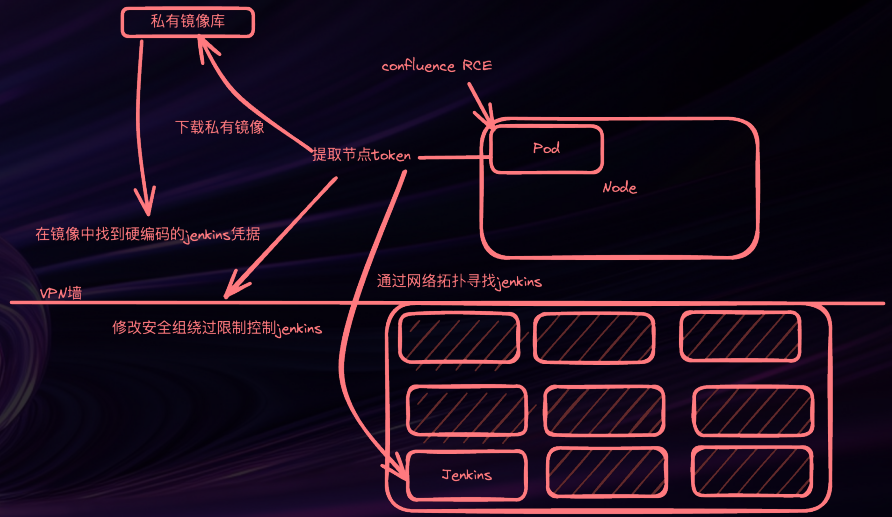
```
AmazonEKSWorkerNodePolicy {
    "Effect":"Allow",
    "Action":[
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcs",
        "eks:Describecluster"
    ]
    "Resource":"*"
}
```

```
AmazonEKS_CNI_Policy {
    "Effect":"Allow",
    "Action":[
        "ec2:AssignPrivateIpAddresses",
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceTypes",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:UnassignPrivateIpAddresses"
    ]
    "Resource":"*"
}
```

获取到一个pod权限后，能做的事情很多

- ✓ 下载所有私有仓库镜像
- ✓ 查看所有镜像漏洞扫描结果
- ✓ 测绘网络拓扑
- ✓ 创建、修改、删除网络接口
- ✓ 修改安全组

案例分析

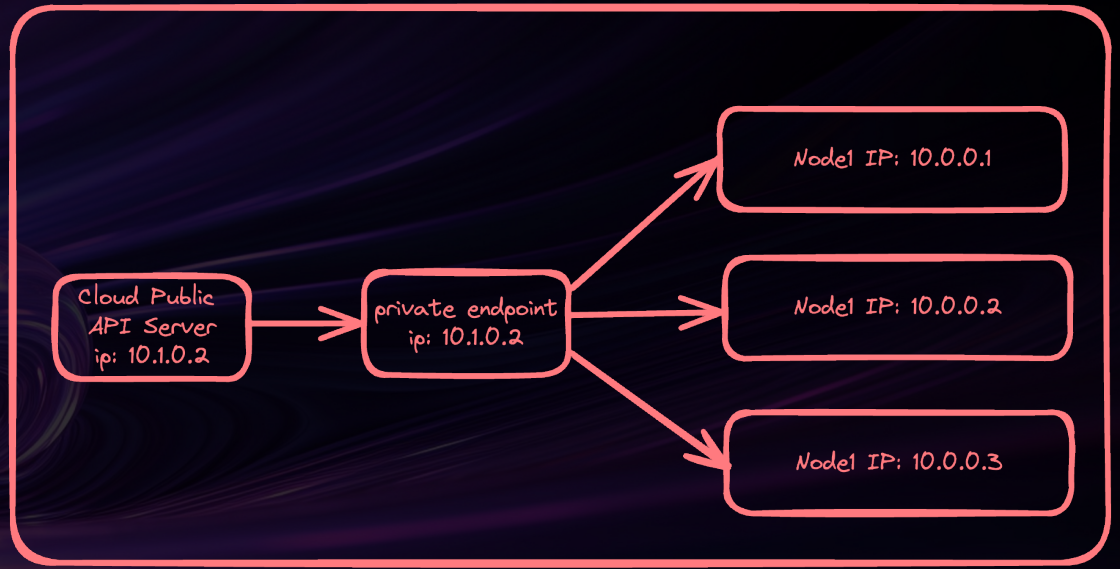

私有镜像库
confluence RCE
下载私有镜像
提取节点token
Pod
Node
在镜像中找到硬编码的jenkins凭据
VPN墙
通过网络拓扑寻找jenkins
修改安全组绕过限制控制jenkins
Jenkins

API滥用提权

Azure常用API

- ✓ listClusterUserCredential
- ✓ listClusterMonitoringUserCredential
- ✓ listClusterAdminCredential
- ✓ listCredential

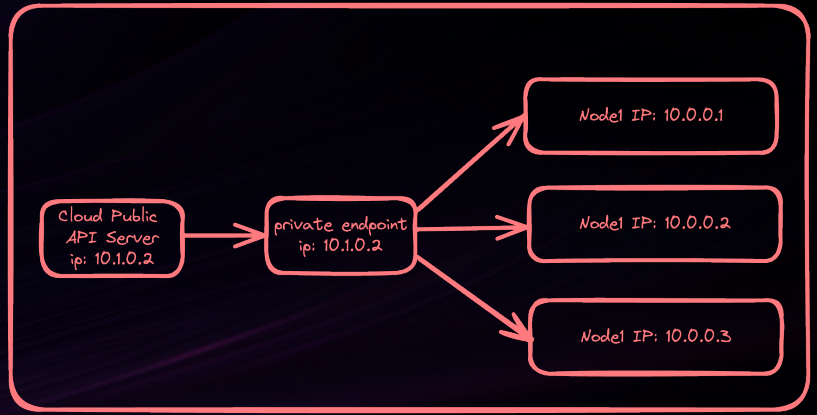
绕过私有集群限制


Cloud Public
API Server
ip: 10.1.0.2
private endpoint
ip: 10.1.0.2
Node1 IP: 10.0.0.1
Node1 IP: 10.0.0.2
Node1 IP: 10.0.0.3

绕过私有集群限制

Runcommand

- ✓ 互联网访问私有集群
- ✓ 所有集群中默认启用
- ✓ 执行命令的Pod默认是以集群管理员形式启动
- ✓ 获取到具有该权限的账户则可控整个集群



Say admin without saying admin

AKS-services role

挖掘类似的风险点是云上攻击的关键所在

/04

攻防启示

庞大且复杂的云原生体系为攻击者提供了更加兴奋的挑战

云原生安全不是黑匣子，了解攻击策略 是构建强防御的第一步

ADCONF

拨云见日
万壑归流

谢谢！