> 问题记录

问题1: 如何确定WAF中需要设置的规则?

答案: 确定WAF（Web应用防火墙）中需要设置的规则通常需要考虑以下几个方面：

通常设置方式包括：

1. **安全需求**: 根据组织的安全策略和业务需求，确定需要保护的Web应用和资源。
2. **合规性**: 确保WAF的规则符合相关的安全标准和法规要求。
3. **攻击检测**: 了解常见的Web应用攻击类型，并设置相应的规则来检测和阻止这些攻击。
4. **性能影响**: 在设置规则时，需要考虑对Web应用性能的影响，避免过度限制合法流量。

结合实际业务场景，可以进一步细化规则设置，例如：

- 通过IP白名单或黑名单来限制对特定资源的访问。（以监控告警为数据来源）
- 对SQL注入、跨站脚本（XSS）等常见攻击进行防护。

问题2: 为什么要将以前的服务迁移到kubernetes上?

答案: 将以前的服务迁移到Kubernetes上可以带来以下几个好处：

- **易于管理**: 传统的服务需要配合配置管理，基础设施管理工具（如Ansible、Puppet等）来管理服务的配置和基础设施。而Kubernetes提供了一个统一的平台来管理应用和服务，简化了配置和管理过程。
- **高可用性**: 通过部署多个Pod副本，Kubernetes可以确保服务在某个节点故障时仍然可用。
- **资源优化**: Kubernetes能够更有效地利用集群资源，避免资源浪费。
- **易于扩展**: 随着业务增长，可以轻松地向Kubernetes集群添加更多节点，以支持更多的应用实例。

问题3: ArgoCD如何实现服务的自动化部署?

答案:

1. 将所有服务的部署配置存放在一个monorepo中，并设置服务的扫描路径
2. 在设置的目录中添加各个服务的applicationset.yaml文件 里面定义服务的helm仓库地址以及相关属性仓库地址
3. 当服务代码发生变化时，通过CI流程触发服务的版本属性仓库，触发应用集的更新，ArgoCD会自动拉取最新的应用集配置并进行部署。
4. 当需要回滚的时候只需要提交一个PR去更新版本属性仓库的版本文件，就能快速的实现回滚。

问题4: 如何在Kubernetes中实现服务的水平扩展?

答案: 在Kubernetes中实现服务的水平扩展通常通过使用Horizontal Pod Autoscaler（HPA）来完成。HPA会根据CPU使用率、内存使用率或其他自定义指标来自动调整Pod的数量，以确保服务能够处理预期的负载。

问题5: 为什么每个账号都用独立的VPC?

答案: 使用独立的VPC（虚拟私有云）为每个账号提供了一系列显著的优势，这些优势有助于提升安全性、管理效率以及资源隔离性：

1. **增强的安全性**： 通过为每个账号分配独立的VPC，可以实现更细粒度的安全策略配置。例如，能够更好地控制入站和出站流量规则，限制不同系统之间的直接访问，减少潜在攻击面，并确保即使在一个VPC内发生安全事件也不会轻易蔓延到其他VPC。
2. **网络隔离与边界清晰化：** 独立的VPC使得各个业务单元或项目之间在网络层面形成严格的逻辑隔离，避免了不必要的交叉干扰。这对于大型组织尤其重要，因为它有助于保持各部门间职责分明，降低误操作风险。
3. **简化管理和维护：** 对于拥有多个部门或者项目的公司而言，在每个账号下创建单独的VPC可以让网络架构更加简洁明了。管理员可以根据具体需求定制每个VPC内的网络设置而不影响其他部分，从而简化整体IT基础设施的管理。
4. **优化成本控制：** 利用AWS等云服务提供商提供的计费模型，企业可以通过将不同的应用部署在各自的VPC中来追踪各个部门或项目的实际消耗情况，进而实现更精准的成本核算与预算规划。
5. **提高灵活性和支持多环境部署：** 当开发团队需要构建测试、预生产及生产等多个运行环境时，使用独立VPC可以方便地复制整个网络结构，快速搭建一致且隔离的运行环境，促进敏捷开发流程并加速产品迭代周期。
6. **符合法规遵从要求：** 某些行业可能对数据存储位置和传输路径有严格规定，而独立VPC可以帮助满足这些合规性需求，比如通过指定特定地理区域内的可用区部署关键工作负载，以确保符合当地法律法规。
综上所述，采用独立VPC的做法不仅增强了系统的安全性与稳定性，同时也为企业提供了更高的运营灵活性和更好的资源管理手段。