保护Kubernetes环境

使用GlobalSign的Atlas颁发Kubernetes证书管理器

mTLS保护业务流程工具
使用可信的mTLS保护pods之间的内部工作负载，以防止攻击并支持“零信任网络”原则

确保kubernetes的安全进入
签发并更新证书，以使用受信任的SSL/TLS安全进入

保护节点和kube API
使用SSL/TLS证书确保Kube API服务器的安全性和完整性

服务的安全性
管理容器化应用程序和服务，确保安全通信和数据保护

kuberenetes的证书管理
在所有Kubernetes环境中标准化证书管理

保持兼容
通过使用公开可信证书确保生产环境的安全性，可以降低中断和入侵相关的风险

由Atlas提供动力
GlobalSign的数字身份平台，一个可信的，可扩展的解决方案

为Kubernetes工作负载构建安全性

根据云原生计算基金会（CNCF），像Kubernetes和容器这样的工具和服务已经在企业中得到了广泛的采用，因此需要使用X.509证书来保护Kubernetes应用程序。手动保护这些身份不再是可持续的，所以使用X.509证书自动化是唯一安全的方法。

cert-manager是最流行的云原生证书管理工具之一，用于保护Kubernetes和OpenShift环境的安全。开发人员使用它从证书颁发机构（CA），如GlobalSign，获得可信的SSL/TLS证书，以保护他们的Kubernetes集群中的应用程序。

使用Kubernetes时最大的安全问题之一是管理端点的错误配置，以及Kubernetes集群中存在的证书缺乏可见性。随着企业开发人员采用一种强调自动化的左移安全管理方法，cert- manager对于使用Kubernetes的企业操作生产环境至关重要。

GlobalSign的Atlas颁发器证书管理器保护Kubernetes的工作负载

GlobalSign的Atlas颁发器证书管理器已经创建，使开发人员能够直接从证书管理器控制器获得公开可信的SSL/TLS证书，以保护Kubernetes集群。它可用于保护各种用例，例如：

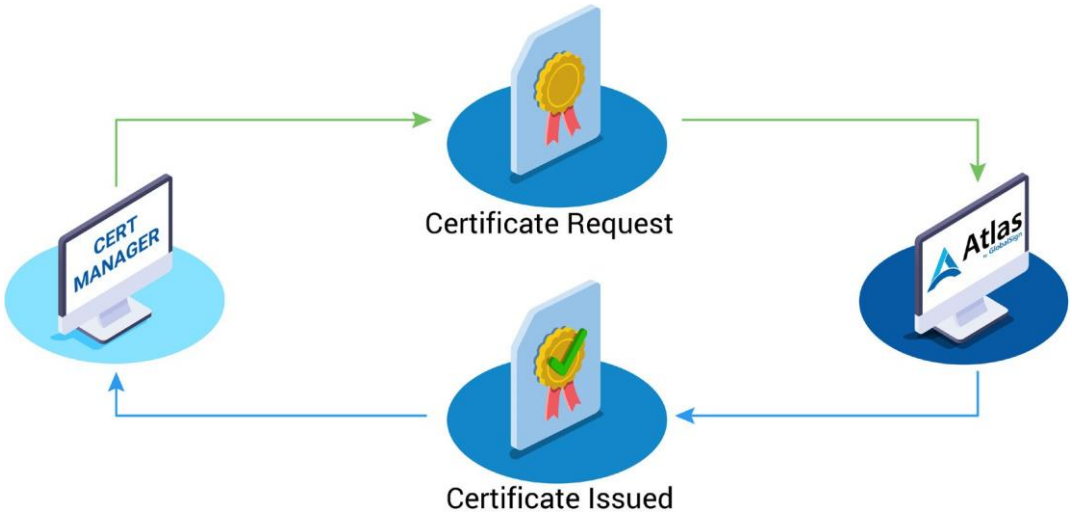
- 使用SSL/TLS证书保护入口
- 使用服务器证书保护Kubelet和Kube API服务器之间的通信
- 使用客户端证书验证Kubelet到API服务器
- 确保舱间通信
- 保护内部web和客户端服务器

工作原理

GlobalSign的Atlas颁发器证书管理器已经创建，开发人员可以直接从证书管理器控制器获取可信的SSL/ TLS证书来保护Kubernetes集群。

获得证书的5个步骤

1. 从GitHub仓库下载并安装GlobalSign的Atlas颁发者cert-manager
2. 从GlobalSign的Atlas门户获取API凭据
3. 使用GlobalSign颁发的API凭据创建颁发者资源
4. 一旦配置好了颁发者资源，为你的Kubernetes资源创建一个证书签名请求（CSR）
5. 一经批准，Atlas将颁发证书



从GlobalSign的发行者开始吧！

从 GlobalSign 的GitHub下载发行者

下载

与你当地的团队取得联系——访问

https://www.globalsign.cn/company/contact

关于GlobalSign

作为全球最具影响力的认证机构之一，GlobalSign是全球领先的可信身份和安全解决方案提供商，使全球的组织、大型企业、云服务提供商和物联网创新者能够进行安全的在线通信，管理数百万已验证数字身份以及自动化认证和加密。其大规模的PKI和身份解决方案支持构成物联网的数十亿项服务、设备、人和物。GMO GlobalSign是日本GMO云KK和GMO互联网集团的子公司，在美洲、欧洲和亚洲设有办事处。

GlobalSign® by GMO