(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 113765899 A
(43)申请公布日 2021.12.07

(21)申请号 202110964781.6

(22)申请日 2021.08.20

(71)申请人 济南浪潮数据技术有限公司
地址 250000 山东省济南市中国(山东)自由贸易试验区济南片区浪潮路1036号浪潮科技园S05楼S311室

(72)发明人 王成龙 崔润兴

(74)专利代理机构 济南诚智商标专利事务所有限公司 37105
代理人 李修杰

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

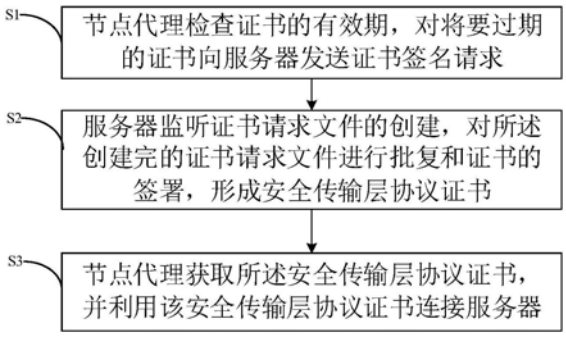
权利要求书2页 说明书4页 附图2页

(54)发明名称

一种节点代理的证书更换方法、系统及装置

(57)摘要

本发明提供了一种节点代理的证书更换方法、系统及装置，所述方法包括节点代理检查证书的有效期，对将要过期的证书向服务器发送证书签名请求；服务器监听证书请求文件的创建，对所述创建完的证书请求文件进行批复和证书的签署，形成安全传输层协议证书；节点代理获取所述安全传输层协议证书，并利用该安全传输层协议证书连接服务器。本发明通过节点代理检查自身证书的有效期，并对即将过期证书发送证书签名请求，在服务器内实现证书的批复及签署，形成安全传输层协议证书，节点代理获取并利用该安全传输层协议证书重新建立与服务器的连接，简化了证书的更换方式，整个过程无需人力参与，极大的节省了人力和时间成本。



CN 113765899 A

1.一种节点代理的证书更换方法,其特征是,所述方法包括以下步骤:

节点代理检查证书的有效期,对将要过期的证书向服务器发送证书签名请求;

服务器监听证书请求文件的创建,对所述创建完的证书请求文件进行批复和证书的签署,形成安全传输层协议证书;

节点代理获取所述安全传输层协议证书,并利用该安全传输层协议证书连接服务器。

2.根据权利要求1所述节点代理的证书更换方法,其特征是,向服务器发送的证书签名请求中包括所述节点代理的单位名称,所述单位名称作为代理标识。

3.根据权利要求2所述节点代理的证书更换方法,其特征是,所述对所述创建完的证书请求文件进行批复和证书的签署具体为:

检测创建完的证书请求文件的标识属性,所述标识属性与代理标识一致时,进行批复;

监听所述证书请求文件的状态,对于批复的证书请求文件进行证书的签署,并将签署的证书附加到证书签名请求中。

4.根据权利要求1所述节点代理的证书更换方法,其特征是,所述证书请求文件的创建通过节点调用API服务器的接口实现。

5.根据权利要求1所述节点代理的证书更换方法,其特征是,所述节点为边缘节点,所述服务器为API服务器。

6.一种节点代理的证书更换系统,其特征是,所述系统包括:

证书检查单元,通过节点代理检查证书的有效期,对将要过期的证书向服务器发送证书签名请求,证书签名请求中包括所述节点代理的单位名称,将所述单位名称作为代理标识;

证书请求文件处理单元,通过服务器监听证书请求文件的创建,对所述创建完的证书请求文件进行批复和证书的签署,形成安全传输层协议证书;

证书更换单元,通过节点代理获取所述安全传输层协议证书,并利用该安全传输层协议证书连接服务器。

7.根据权利要求6所述节点代理的证书更换系统,其特征是,所述证书请求文件处理单元包括:

批复模块,用于检测创建完的证书请求文件的标识属性,所述标识属性与代理标识一致时,进行批复;

签名模块,用于监听所述证书请求文件的状态,对于批复的证书请求文件进行证书的签署,并将签署的证书附加到证书签名请求中。

8.一种节点代理的证书更换装置,包括节点代理和服务器,其特征是,所述节点代理检查证书的有效期,对将要过期的证书向服务器发送证书签名请求,并获取服务器基于所述证书签名请求形成的安全传输层协议证书,利用该安全传输层协议证书连接服务器;所述服务器监听证书请求文件的创建,对所述创建完的证书请求文件进行批复和证书的签署,形成安全传输层协议证书;所述证书签名请求中包括所述节点代理的单位名称,所述单位名称作为代理标识。

9.根据权利要求8所述节点代理的证书更换装置,其特征是,所述服务器包括批复控制器和签名控制器;

所述批复控制器,检测创建完的证书请求文件的标识属性,所述标识属性与代理标识

一致时,进行批复;

所述签名控制器,监听所述证书请求文件的状态,对于批复的证书请求文件进行证书的签署,并将签署的证书附加到证书签名请求中。

10.一种计算机存储介质,所述计算机存储介质中存储有计算机指令,其特征是,所述计算机指令在权利要求6或7所述系统上运行时,使所述系统执行如权利要求1-5任一项所述方法的步骤。

一种节点代理的证书更换方法、系统及装置

技术领域

[0001] 本发明涉及集群安全技术领域，尤其是一种节点代理的证书更换方法、系统及装置。

背景技术

[0002] 容器技术是一种比虚拟机技术更加节省计算资源也更加灵活的虚拟化技术。随着容器技术的发展，出现了很多容器编排引擎，用于对容器进行管理，Kubernetes(用于自动部署，扩展和管理容器化应用程序的开源系统)技术脱颖而出成为了容器编排领域的事实标准。

[0003] 随着云原生技术的逐步成熟，将Kubernetes系统延展到边缘计算场景，边缘节点通过公网和中心云连接，为了保证通信的安全需要要使用基于HTTPS(Hyper Text Transfer Protocol over SecureSocket Layer，以安全为目标的HTTP通道)的加密协议。

[0004] HTTPS建立连接的阶段是非对称加密+对称加密+数字证书协同作用的过程。但是数字证书是有时间限制的，一旦过期HTTPS将不能继续建立连接进行通信，因此需要定时进行证书的更换，证书的更新轮换将给企业带来很大的人力维护以及时间成本。

发明内容

[0005] 本发明提供了一种节点代理的证书更换方法、系统及装置，用于解决现有证书更新轮换给企业带来大量时间和人力成本的问题。

[0006] 为实现上述目的，本发明采用下述技术方案：

[0007] 本发明第一方面提供了一种节点代理的证书更换方法，所述方法包括以下步骤：

[0008] 节点代理检查证书的有效期，对将要过期的证书向服务器发送证书签名请求；

[0009] 服务器监听证书请求文件的创建，对所述创建完的证书请求文件进行批复和证书的签署，形成安全传输层协议证书；

[0010] 节点代理获取所述安全传输层协议证书，并利用该安全传输层协议证书连接服务器。

[0011] 进一步地，向服务器发送的证书签名请求中包括所述节点代理的单位名称，所述单位名称作为代理标识。

[0012] 进一步地，所述对所述创建完的证书请求文件进行批复和证书的签署具体为：

[0013] 检测创建完的证书请求文件的标识属性，所述标识属性与代理标识一致时，进行批复；

[0014] 监听所述证书请求文件的状态，对于批复的证书请求文件进行证书的签署，并将签署的证书附加到证书签名请求中。

[0015] 进一步地，所述证书请求文件的创建通过节点调用API服务器的接口实现。

[0016] 进一步地，所述节点为边缘节点，所述服务器为API服务器。

[0017] 本发明第二方面提供了一种节点代理的证书更换系统，所述系统包括：

[0018] 证书检查单元，通过节点代理检查证书的有效期，对将要过期的证书向服务器发送证书签名请求，证书签名请求中包括所述节点代理的单位名称，将所述单位名称作为代理标识；

[0019] 证书请求文件处理单元，通过服务器监听证书请求文件的创建，对所述创建完的证书请求文件进行批复和证书的签署，形成安全传输层协议证书；

[0020] 证书更换单元，通过节点代理获取所述安全传输层协议证书，并利用该安全传输层协议证书连接服务器。

[0021] 进一步地，所述证书请求文件处理单元包括：

[0022] 批复模块，用于检测创建完的证书请求文件的标识属性，所述标识属性与代理标识一致时，进行批复；

[0023] 签名模块，用于监听所述证书请求文件的状态，对于批复的证书请求文件进行证书的签署，并将签署的证书附加到证书签名请求中。

[0024] 本发明第三方面提供了一种节点代理的证书更换装置，包括节点代理和服务器，所述节点代理检查证书的有效期，对将要过期的证书向服务器发送证书签名请求，并获取服务器基于所述证书签名请求形成的安全传输层协议证书，利用该安全传输层协议证书连接服务器；所述服务器监听证书请求文件的创建，对所述创建完的证书请求文件进行批复和证书的签署，形成安全传输层协议证书；所述证书签名请求中包括所述节点代理的单位名称，所述单位名称作为代理标识。

[0025] 进一步地，所述服务器包括批复控制器和签名控制器；

[0026] 所述批复控制器，检测创建完的证书请求文件的标识属性，所述标识属性与代理标识一致时，进行批复；

[0027] 所述签名控制器，监听所述证书请求文件的状态，对于批复的证书请求文件进行证书的签署，并将签署的证书附加到证书签名请求中。

[0028] 本发明第四方面提供了一种计算机存储介质，所述计算机存储介质中存储有计算机指令，所述计算机指令在所述系统上运行时，使所述系统执行所述方法的步骤。

[0029] 本发明第二方面的所述证书更换系统和第三方面所述的证书更换装置均能够实现第一方面及第一方面的各实现方式中的方法，并取得相同的效果。

[0030] 发明内容中提供的效果仅仅是实施例的效果，而不是发明所有的全部效果，上述技术方案中的一个技术方案具有如下优点或有益效果：

[0031] 本发明通过节点代理检查自身证书的有效期，并对即将过期证书发送证书签名请求，在服务器内实现证书的批复及签署，形成安全传输层协议证书，节点代理获取并利用该安全传输层协议证书重新建立与服务器的连接，简化了证书的更换方式，整个过程无需人力参与，极大的节省了人力和时间成本。

附图说明

[0032] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，对于本领域普通技术人员而言，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0033] 图1是本发明所述方法的流程示意图；

[0034] 图2是本发明所述方法具体实现过程示意图；

[0035] 图3是本发明所述系统的结构示意图；

[0036] 图4是本发明所述装置的工作原理示意图。

具体实施方式

[0037] 为能清楚说明本方案的技术特点，下面通过具体实施方式，并结合其附图，对本发明进行详细阐述。下文的公开提供了许多不同的实施例或例子用来实现本发明的不同结构。为了简化本发明的公开，下文中对特定例子的部件和设置进行描述。此外，本发明可以在不同例子中重复参考数字和/或字母。这种重复是为了简化和清楚的目的，其本身不指示所讨论各种实施例和/或设置之间的关系。应当注意，在附图中所图示的部件不一定按比例绘制。本发明省略了对公知组件和处理技术及工艺的描述以避免不必要地限制本发明。

[0038] 如图1所示，本发明一种节点代理的证书更换方法，包括以下步骤：

[0039] S1，节点代理检查证书的有效期，对将要过期的证书向服务器发送证书签名请求；

[0040] S2，服务器监听证书请求文件的创建，对所述创建完的证书请求文件进行批复和证书的签署，形成安全传输层协议证书；

[0041] S3，节点代理获取所述安全传输层协议证书，并利用该安全传输层协议证书连接服务器。

[0042] 步骤S1中，向服务器发送的证书签名请求中包括所述节点代理的单位名称，所述单位名称作为代理标识。

[0043] 步骤S2中，所述对所述创建完的证书请求文件进行批复和证书的签署具体为：检测创建完的证书请求文件的标识属性，所述标识属性与代理标识一致时，进行批复；监听所述证书请求文件的状态，对于批复的证书请求文件进行证书的签署，并将签署的证书附加到证书签名请求中。其中对证书请求文件的批复通过服务器内的批复控制器实现；证书的签署通过服务器内的签名控制器实现。

[0044] 所述证书请求文件的创建通过节点调用API服务器的接口实现。

[0045] 如图2所示，本发明实现上述方法的具体过程如下，其中所述节点为边缘节点，所述服务器为API服务器Kubernetes APIServer。

[0046] 1)、边缘节点代理定时检查证书的日期。

[0047] 2)边缘节点代理对于即将过期证书向Kubernetes APIServer发送证书签名请求CSR(Certificate Signing Request)，CSR中包含公钥和代理标识，本实施例中将代理的Organization作为代理标识。

[0048] 3)批复控制器对满足条件的CSR进行批复，其中满足条件是指创建的证书请求文件中存在与代理标识一致的标识属性。

[0049] 4)向Kubernetes APIServer返回批复结果。

[0050] 5)签名控制器对已批复的CSR进行证书签署。

[0051] 6)签名控制器将签署的证书附件到证书签名请求中。

[0052] 7)边缘节点代理向Kubernetes APIServer请求获取签署的证书。

[0053] 8)Kubernetes APIServer向边缘节点代理返回签署的安全传输层协议证书TLS。

[0054] 9)边缘节点代理将TLS证书写入磁盘，进行证书轮换。

[0055] 10)关闭之前的连接,并更新与Kubernetes APIServer的连接,使用新的证书重新连接到Kubernetes APIServer。

[0056] 如图3所示,本发明还提供了一种节点代理的证书更换系统,所述系统包括证书检查单元1、证书请求文件处理单元2和证书更换单元3。

[0057] 证书检查单元1通过节点代理检查证书的有效期,对将要过期的证书向服务器发送证书签名请求,证书签名请求中包括所述节点代理的单位名称,将所述单位名称作为代理标识;证书请求文件处理单元2通过服务器监听证书请求文件的创建,对所述创建完的证书请求文件进行批复和证书的签署,形成安全传输层协议证书;证书更换单元3通过节点代理获取所述安全传输层协议证书,并利用该安全传输层协议证书连接服务器。

[0058] 所述证书请求文件处理单元包括批复模块21和签名模块22。

[0059] 批复模块21用于检测创建完的证书请求文件的标识属性,所述标识属性与代理标识一致时,进行批复;签名模块22用于监听所述证书请求文件的状态,对于批复的证书请求文件进行证书的签署,并将签署的证书附加到证书签名请求中。

[0060] 如图4所示,本发明的一种节点代理的证书更换装置,包括节点代理和服务器Kubernetes APIServer。边缘节点通过公网与中心云连接。服务器包括批复控制器和签名控制器。

[0061] 所述节点代理通过定时器定时检查证书是否过期,对将要过期的证书向服务器发送证书签名请求CSR;所述服务器监听证书请求文件CSR的创建,批复控制器检测创建完的证书请求文件的标识属性,所述标识属性与代理标识一致时,进行批复;签名控制器监听所述证书请求文件的状态,对于批复的证书请求文件进行证书的签署,并将签署的证书附加到证书签名请求中,形成安全传输层协议证书TLS。

[0062] 代理获取服务器基于所述证书签名请求形成的安全传输层协议证书TLS写入磁盘,进行证书轮换,利用该安全传输层协议证书建立与服务器的HTTPS连接;

[0063] 本发明还提供了一种计算机存储介质,所述计算机存储介质中存储有计算机指令,所述计算机指令在所述系统上运行时,使所述系统执行所述方法的步骤。

[0064] 上述虽然结合附图对本发明的具体实施方式进行了描述,但并非对本发明保护范围的限制,所属领域技术人员应该明白,在本发明的技术方案的基础上,本领域技术人员不需要付出创造性劳动即可做出的各种修改或变形仍在本发明的保护范围以内。

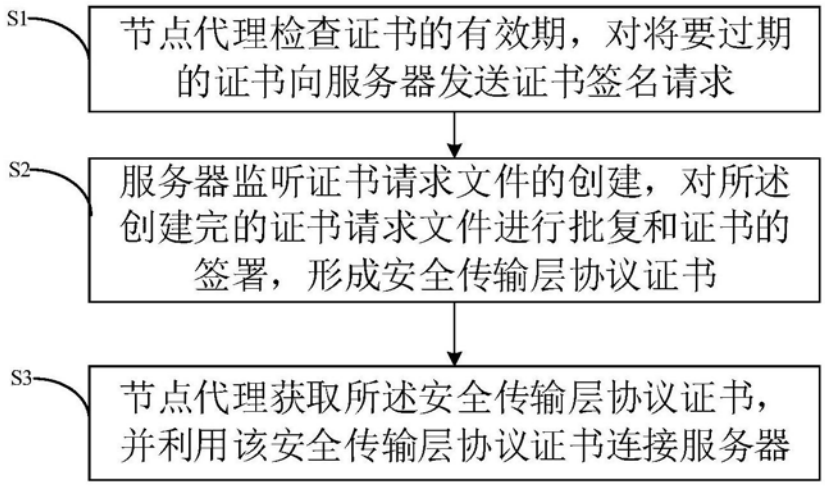

S1
节点代理检查证书的有效期，对将要过期的证书向服务器发送证书签名请求
S2
服务器监听证书请求文件的创建，对所述创建完的证书请求文件进行批复和证书的签署，形成安全传输层协议证书
S3
节点代理获取所述安全传输层协议证书，并利用该安全传输层协议证书连接服务器

图1

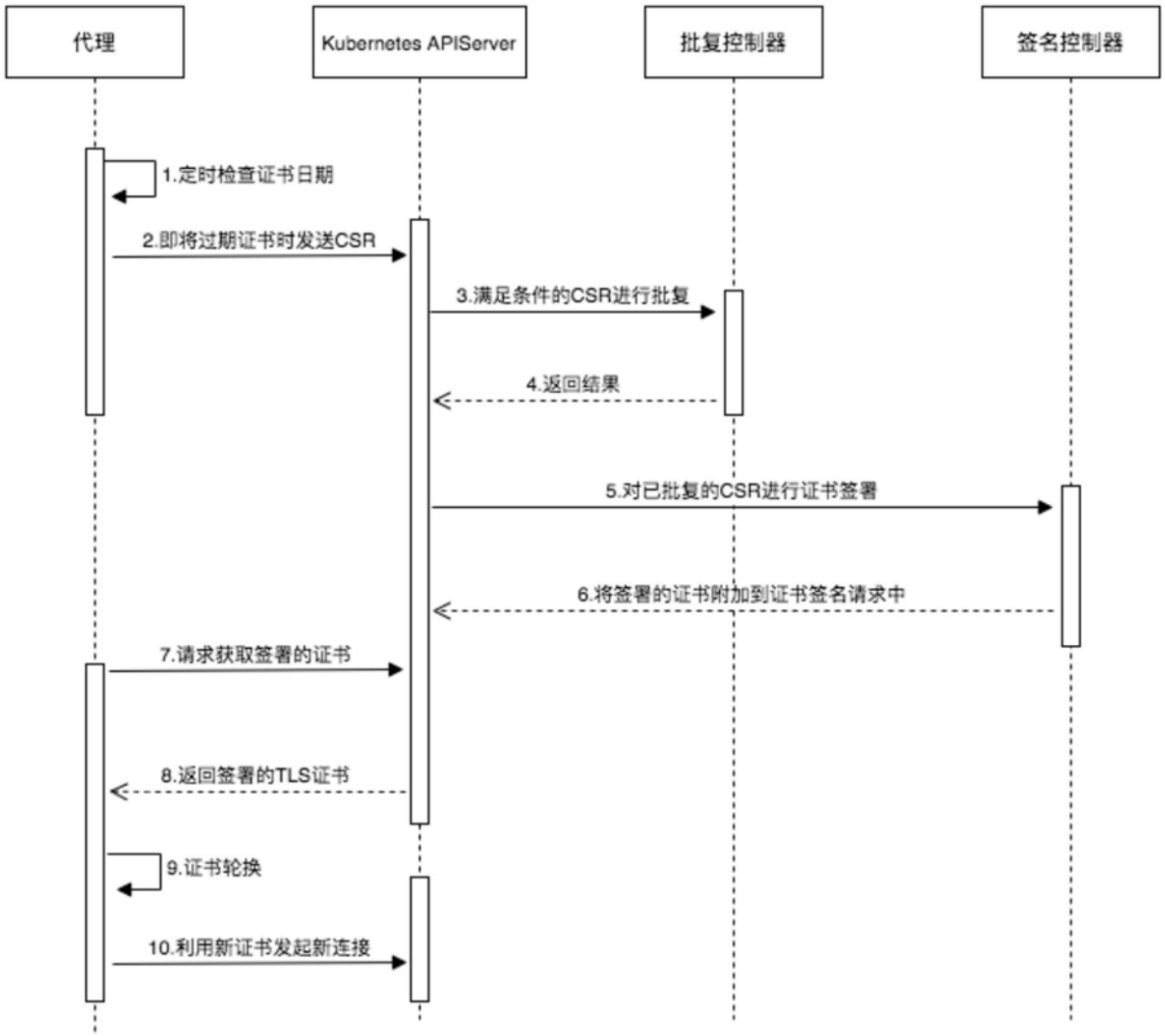

代理
Kubernetes APIServer
批复控制器
签名控制器
1.定时检查证书日期
2.即将过期证书时发送CSR
3.满足条件的CSR进行批复
4.返回结果
5.对已批复的CSR进行证书签署
6.将签署的证书附加到证书签名请求中
7.请求获取签署的证书
8.返回签署的TLS证书
9.证书轮换
10.利用新证书发起新连接

图2

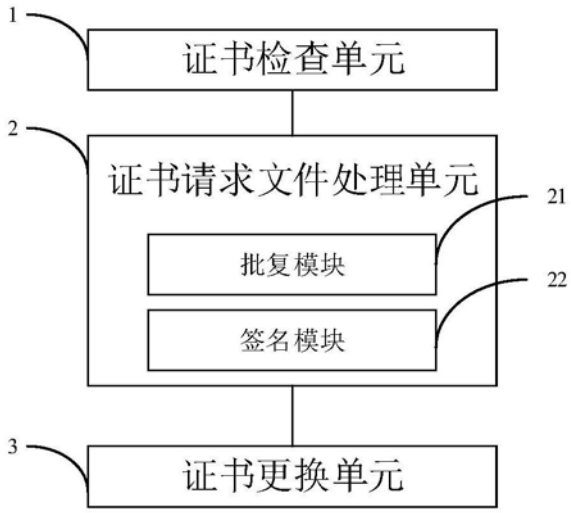

1
证书检查单元
2
证书请求文件处理单元
21
批复模块
22
签名模块
3
证书更换单元

图3

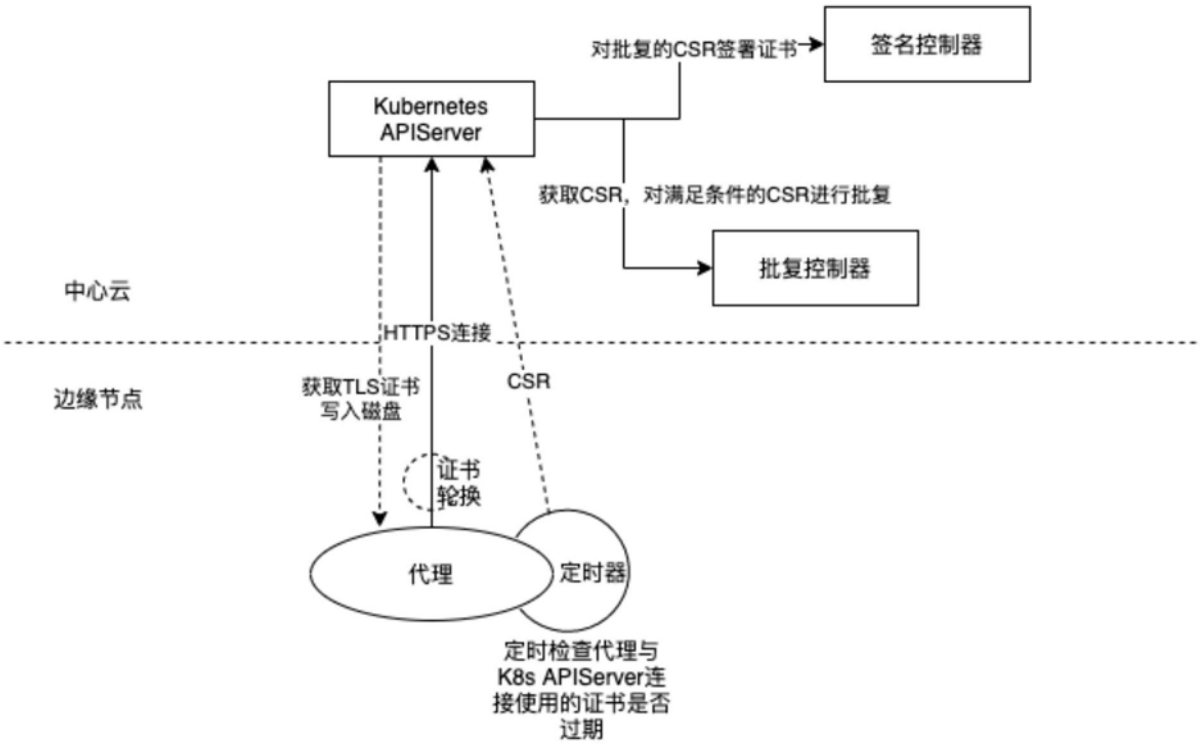

对批复的CSR签署证书
签名控制器
Kubernetes APIServer
获取CSR，对满足条件的CSR进行批复
批复控制器
中心云
HTTPS连接
边缘节点
获取TLS证书写入磁盘
CSR
证书轮换
代理
定时器
定时检查代理与K8s APIServer连接使用的证书是否过期

图4