

OpenStack 认证安全问题研究

Research on OpenStack Identification Security Issues

熊 微¹,房秉毅¹,张云勇¹,吴 俊²,李素粉¹(1. 中国联通研究院,北京 100048;2. 北京邮电大学,北京 100876)

Xiong Wei¹,Fang Bingyi¹,Zhang Yunyong¹,Wu Jun²,Li Sufen¹(1. China Unicom Research Institute,Beijing 100048,China;2. Beijing University of Posts and Telecommunications,Beijing 100876,China)

摘 要:

选择 Keystone 组件作为 OpenStack 安全问题研究的切入点,分析了该组件相关的安全问题。首先简要介绍了 OpenStack 的主要功能组件及组件间的交互关系,详细描述了 Keystone 的对象模型,并深入研究了其认证机制。在充分分析了 Keystone 运行机制的基础上,提出了 Keystone 中存在的安全问题,并给出了相应的改进方案。

关键词:

云计算;安全;OpenStack

中图分类号:TP939

文献标识码:A

文章编号:1007-3043(2014)07-0021-05

Abstract:

Selecting Keystone component as the beginning of researching OpenStack security issues, it analyzes the security issues on this component. It firstly describes the major functional components of OpenStack and the interactive relation between the components, presents object model of Keystone in detail, and researches its identification mechanism. Based on the analysis of Keystone operation mechanism, it presents the security issues on Keystone and gives the relative improvement solution.

Keywords:

Cloud computing; Security; OpenStack

0 前言

OpenStack 是一个由 Rackspace 和 NASA 发起、全球开发者共同参与的开源项目,旨在打造容易部署、功能丰富且易于扩展的云计算平台,它可以为用户提供类似 Amazon Web Service 的服务。到目前为止,OpenStack 已经发布了 8 个版本,其系统功能在版本演进的过程中得到了不断的完善,以安全功能方面的认证授权功能为例,在 Essex 版本之前,OpenStack 的各个子项目如 Nova、Swift 均使用各自独立的认证系统,Swift 组件中使用一种名为“swauth”的身份验证和用户

授权方法,从 Essex 版本之后开始全面支持 Keystone。OpenStack 作为开源云平台,虽然有良好的跟踪记录,但是仍存在漏洞和脆弱性,其安全问题也是作为 OpenStack 发展过程中需重点考虑的问题之一。OpenStack 安全组织及相关研究人员在 OpenStack 安全研究方面进行了积极探索。OpenStack 安全组在其发布的[安全指南](#)^[1]中明确指出了 OpenStack 的安全范围,该指南指出了 OpenStack 的用户和实施者在使用过程中存在各种安全痛点,但是并没有直接解决 OpenStack 中的安全漏洞。Cooper J D^[2]以 OpenStack 作为研究案例,对云平台的安全特征进行了研究,识别与授权和身份管理、数据管理相关的安全漏洞,并针对所发现的问题,提供不同的建议去解决这些问题。Ristov S^[3]分析了私有或公有网络的安全漏洞,针对虚拟机实例和 OpenStack 云节点,提出了 3 个假设并验证其正确性。相关的 OpenStack 安全方面的研究工作主要是从云平

基金项目:国家自然科学基金资助项目(71172134);国家科技重大基金资助项目(2012ZX03002001-002、2013ZX03002004-002、2013ZX03002003-005)

收稿日期:2014-05-29

台的整体安全性角度出发,给出部分组件中存在的漏洞,提出改进的方向或建议,并没有针对某个特定的功能组件展开深入的研究。

1 OpenStack 系统框架

OpenStack 是一个纯 IaaS 交付模型,任何组织均可以通过 OpenStack 基于标准化的硬件设施创建和提供云计算服务。OpenStack 的主要 7 个核心组件关系如图 1 所示。

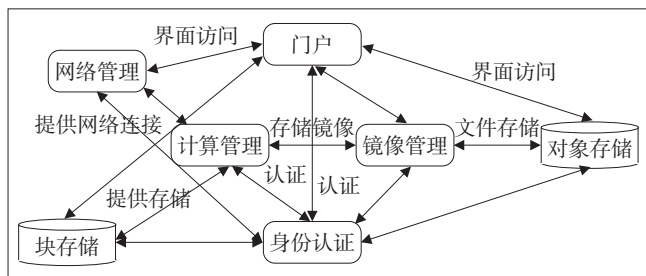


图1 OpenStack 核心系统架构

计算管理(Nova):提供虚拟主机,对应亚马逊的 EC2,包括虚拟机、弹性云硬盘等。通过虚拟化技术(如 KVM、Xen、VMware Esxi 等实现计算、网络、存储等资源池的构建及应用),将计算能力通过虚拟机的方式交付用户。

镜像管理(Glance):提供虚拟磁盘镜像的目录分类管理以及镜像库存储管理。

身份认证(Keystone):为 OpenStack 所有的系统提供统一的授权和身份验证。

网络管理(Quantum):实现了虚拟机的网络资源管理,包括网络连接、子网 IP 管理、L3 的公网映射、后续的负载均衡等。Folsom 版中的 Quantum 对应于 Essex 版中 Nova 中的 nova-network。

对象存储(Swift):对应亚马逊的 S3,通过简单 key/value 的方式实现对象文件的存储读取。

块存储(Cinder):与亚马逊的 EBS 弹性云硬盘类似,实现了对块存储的管理,为虚拟机提供云硬盘服务。在 Essex 版本中是由 nova-volume 实现块存储的管理,在 Folsom 版本之后,独立新增的 Cinder 项目增强了块存储方面的管理能力。

门户(Horizon):基于 OpenStack API 接口开发的 Web 呈现。

从图 1 可以看出 OpenStack 所有模块系统之间都是通过标准的 API 接口进行服务调用,因此所有涉及服务 API 的调用都脱离不了 Keystone。Keystone 为

OpenStack 所有的系统提供统一的授权和身份认证服务,负责身份验证、服务规则和服务令牌的功能,它实现了 OpenStack 的 Identity API,其他服务需要通过 Keystone 来注册其服务的 Endpoint(服务访问的 URL),任何服务之间相互的调用,都需要经过 Keystone 进行身份验证,来获得目标服务的 Endpoint,从而找到目标服务。Keystone 作为 OpenStack 身份验证的中央安全中心,其安全问题将直接影响着其他模块子系统的安全。下面就对 Keystone 的运行机制及其安全问题进行分析和介绍。

2 Keystone 运行机制分析

Keystone 使用基于 Token/PKI 的身份认证机制提供单点登录认证和访问控制服务。身份认证服务提供 2 个功能:用户管理、追踪用户及其许可和服务目录,提供可用服务的目录及其 API 端点。OpenStack 所有组件都依赖于 Keystone 提供 3A (Account、Authentication、Authorization) 服务。除了 3A 之外,Keystone 还对外提供服务目录(Service Catalog)服务,用户(无论是 Dashboard 还是 API Client)都需要访问 Keystone 获取服务列表以及每个服务的地址(OpenStack 中称为 Endpoint)。OpenStack 身份管理是基于标准 PKI 功能的令牌,允许客户端无须身份服务呼叫便可获取离线令牌认证。OpenStack 身份管理还针对多租户环境提供了更为系统化的管理能力,支持群组、角色扮演、角色接入控制(RBAC),赋予管理员更大的权力。

2.1 Keystone 对象模型

在介绍 Keystone 对象模型之前,先要介绍一下 Keystone 中的几个基本概念。

a) 用户(User):数字代表了使用 OpenStack 云服务的人、系统或服务。身份验证服务会验证传入的请求。用户有可能被分配一个登录名和令牌来访问资源,并标识其为 API 的一个特定使用者,属于一个指定的域。同时,可以赋予用户角色,每一个用户域或用户项目都可以有一组角色。

b) 证书(Credential):保证数据只有能证明他们是谁的用户知道。例如,用户名和密码、用户名和 API 密钥或由身份认证服务提供的身份认证令牌。它也是与用户关联的认证凭据。一个用户可能有一个或多个证书,一个证书与某一个项目关联。

c) 令牌(Token):用于访问资源的任意字节的文本。每个令牌都有一个范围,该范围描述了这个令牌

所能访问的资源。一个令牌可以随时被取消,其有效性为有限的持续时间。Keystone通过验证一组由用户提供的证书来验证出入的请求,为了响应这些证书,Keystone为用户发布一个身份验证令牌,用户在随后的请求中需要提供该令牌。

d) 组(Group):表示一组拥有某权限的用户,属于一个指定的域。可以赋予组特定的角色,此时组内的用户会被赋予该角色所具有的权限。

e) 域(Domain):表示一组项目和用户的集合。每一个项目或用户只能属于一个域,但用户可以属于多个项目。域有命名空间的概念,即在一个命名空间内的名称是否是全局唯一。

f) 租户/项目(Tenant/Project):在 OpenStack 中表示一组资源(在 Folsom 版本中叫 Tenant,在 Grizzly 版中叫 Project),是一个用户分组或隔离资源/身份对象的容器,一个项目属于某一个域。

g) 角色(Role):表示一组项目或者域范围内所允许的操作。一个角色包含一组权利和特权。在认证服务中,分发给用户的令牌包含用户拥有的角色列表。用户所能调用的服务能表明用户所拥有角色的集合,以及每个角色能够访问的资源 and 操作。

上述的主要对象之间的关系模型如图2所示。

2.2 Keystone 认证机制

OpenStack 中身份认证分为2个部分:首先,用户进行初始化身份认证时,会为用户分配一个Token;然

后使用该Token进行单点登录和委派验证。下面介绍 OpenStack 中Token的工作原理。OpenStack 在 G 版之前使用的是 UUID Token,在 G 版之后引入新的方法验证Token,这是因为 PKI(Public Key Infrastructure)能够增强第一步中的安全性,同时也能提高第二步中的安全性和扩展性。

2.2.1 UUID Token

OpenStack 在 G 版之前使用的是 UUID Token,图3显示了 Keystone 是如何生成Token及用户是如何利用Token“签署”每一个后续API请求的过程。

基于提供的用户名/密码对(假设它在这个场景和图3中是正确的),生成1个UUID Token过程如下。

- 在 Keystone 的后端存储 UUID Token。
- 将 UUID Token 的拷贝发送给用户。
- 用户缓存Token到本地。
- UUID将会和用户发起的每个API调用一起传递。
- 基于每个用户的请求,API端点会将这个UUID传回给 Keystone 去验证。
- Keystone 会拿 UUID 与其授权后台匹配(检查 UUID 字符串和失效日期)。
- Keystone 会给API端点返回“成功”或“失败”消息。

从图3可知,对每个用户调用API端点需要使用 Keystone 服务执行在线验证。假设上千个用户执行 VM listings、网络创建等,这样就会导致为 Keystone 服务扩大流量。

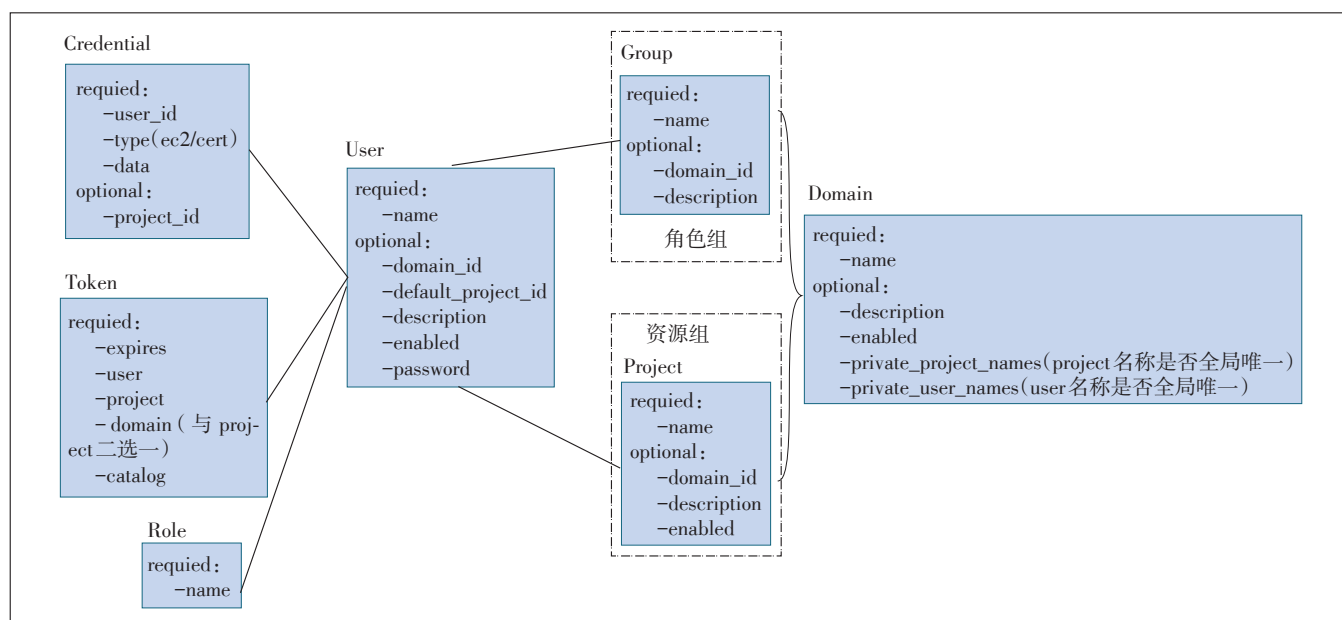


图2 Keystone对象关系模型

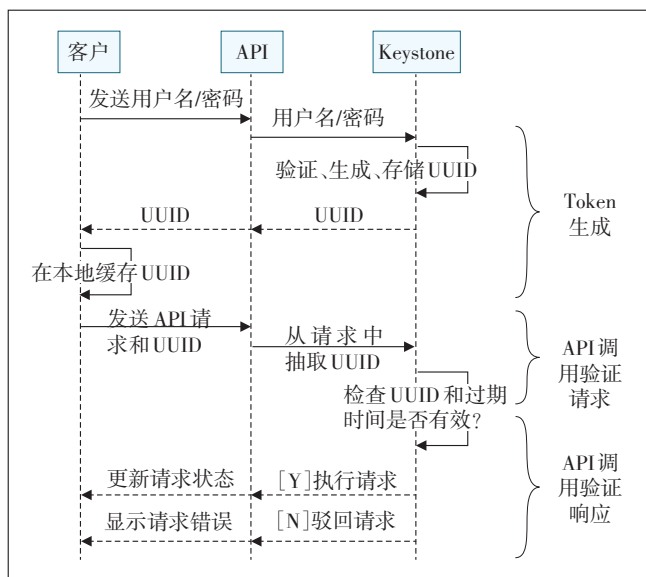


图3 UUID Token 过程

2.2.2 PKI Token

OpenStack 在 Grizzly 版中引入的新方法验证 Token (见图4)。

概括地说,使用 PKI Token,Keystone 逐渐成为一个数字签名认证中心(CA)。它使用签名密钥和数字证书来签名用户的 Token。每个 API 端点持有一份 Keystone 的拷贝,包括签名证书、撤销列表、CA 数字签

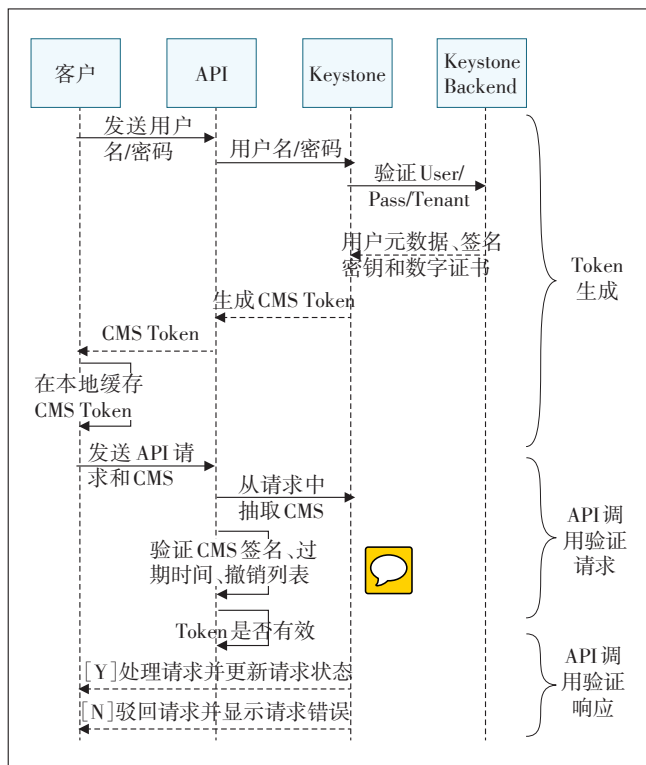


图4 PKI Token 过程

名。API 端点使用这些字节来验证用户的请求。没有必要为每个验证直接请求 Keystone。签名 Keystone 放在用户令牌和 Keystone 的撤销列表。API 端点使用以上数据离线地执行这个过程。

3 Keystone 中的安全问题及改进方案

通过本文第2章中对 Keystone 安全机制的介绍和研究,本章主要是识别目前 OpenStack 认证机制中存在的问题,针对其进行分析,并给出了改进的方向。

3.1 Keystone 中的安全问题

a) OpenStack 使用 Keystone 作为身份验证的中央安全中心。身份验证机制是基于用户名和密码,以明文的形式发送,当身份验证成功后,Keystone 服务器生成一个有效 Token,终端用户通过它来获得服务。此外,所有的通信通过 HTTP 协议执行,因此可能会存在对用户名和密码、通信协议方面的攻击。

b) 即使在 OpenStack 的 Gizzly 版中,Keystone 也并不提供在重复登录失败后限制登录的方法。重复失败登录有可能是在进行暴力攻击 brute-force attacks,可以通过使用一个外部的身份验证系统。

c) OpenStack 使用密码用于身份验证且以明文的形式发送。使用 HTTP 通信协议来进行授权,相比之下,没有 HTTPS 安全。生成的身份验证的 Token 不是一个证书,仅有 32 bit 长。此外,Token 的生命周期很短,默认是 24 h,这意味着用户在 Token 过期后需要重新进行身份认证。在 Keystone 中实施 PKI,可以生成证书,其有效期会更长。在身份验证成功后且在 Token 的有效期内,每个服务都必须借助 Keystone 来确认 Token 的可靠性,这可能会引发扩展性方面的问题。32 位 Token 生成的随机性仍然是个问题。作为一个单点故障,Keystone 仍然是认证和授权的瓶颈。

3.2 Keystone 安全改进方案

3.2.1 基于 PKI 扩展 OpenStack 弱认证

PKI 可以在 Keystone 中单独实施,然而,撤销和可扩展性是很重要的方面。这意味着一个单独的证书颁发机构,例如需要“中央安全服务器”来处理认证请求,并为 Keystone 提供有效的证书。此外,在 OpenStack 中使用 Keystone 进行认证分两步:首先,需要用户名和密码、成功的认证、Keystone 生成一个有效的 Token;然后使用这个有效的 Token 来提供单点登录(SSO)和委托认证。实施 PKI 能够提高第一步中的安全性,可以通过提供签名认证和授权 Token 来增强第二步中的安全

性和可扩展性。

图5示出的是基于PKI的初始化认证。

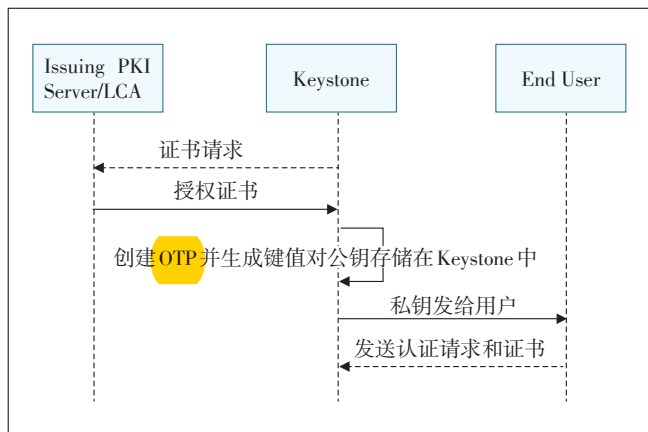


图5 基于PKI的初始化认证

3.2.2 代理授权

Keystone 在线验证Token和租户需要用户的积极参与,但是通过实施PKI,可以提高包含认证和授权信息的Token的安全性和可扩展性。通过密码签名和Keystone的私钥对Token的信息内容加密,确保那些有Keystone公钥的服务才能解密信息。因此,也就减少了Token验证对网络的需求及去Keystone中获取角色信息的需求。整个方法包括将Token认证中间件修改为基于Token的CMS (Cryptographic Message Syntax)。这种代理授权的方法仅能用于OpenStack部署中。由于消息签名需要用户的私钥,而用户私钥并非由Keystone模块自己维护,当前的浏览器并不支持代表一个网站去签名消息,门户(Dashboard)需要的代理授权其实代表的是已登录系统的用户。这意味着用户必须首先使用他的证书登录到门户,然后使用Keystone Token进行委托授权。

图6示出的是认证和委托协议。

4 结束语

本文对Keystone安全机制的分析和研究是基于比

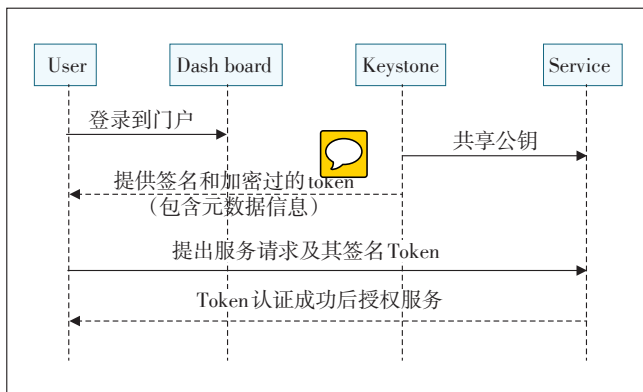


图6 认证和委托协议

较新的2个版本,即F版和G版。本文深入研究了OpenStack中的Keystone对象,对Keystone的安全研究着重于基于Token/PKI授权。通过研究其对象模型和认证机制,分析了Keystone中存在的安全问题,并给出相应的改进方案。

参考文献:

- [1] The OpenStack Security Group. OpenStack Security Guide [EB/OL]. [2013-11-20]. <http://docs.openstack.org/security-guide/content/>.
- [2] Cooper J D. Analysis of security in cloud platforms using OpenStack as case study [EB/OL]. [2013-11-20]. <http://brage.bibsys.no/xmlui/bitstream/handle/11250/137588/Cooper,%20John%20David%20ppgave.pdf?sequence=1>.
- [3] Ristov S, Gusev M, Donevski A. OpenStack Cloud Security Vulnerabilities from Inside and Outside [C]//CLOUD COMPUTING 2013, The Fourth International Conference on Cloud Computing, GRIDs, and Virtualization, 2013: 101-107.

作者简介:

熊微,硕士,主要从事云计算相关技术的研究;房秉毅,高级工程师,博士,主要从事云计算、核心网新技术的研究;张云勇,中国联通研究院平台与云计算研究中心主任,博士后,主要研究方向为下一代开放网络、固定移动融合核心网、移动互联网及业务、公共运算;吴俊,副教授,博士,IEEE/AIS/PMI高级会员,主要研究方向为移动互联网应用、云计算商业价值评价等;李素粉,博士,主要从事云计算相关技术的研究。

广告索引

封一 华为技术有限公司

封二 烽火通信科技股份有限公司

封三 2014中国国际信息通信展览会

封四 双登集团股份有限公司

前插1 江苏亨通光电股份有限公司

前插2 2014联通论坛

前插3 河北先控捷联电源设备有限公司

前插4 上海贝尔股份有限公司

前插5 中讯邮电咨询设计院有限公司

目录广告1 江苏亨通光电股份有限公司

目录广告2 厦门科华恒盛股份有限公司