弹性云服务器

QingTian 系统安全技术白皮书

文档版本 01

发布日期 2025-10-17

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 QingTian 系统安全技术白皮书

1.1 引言

华为云弹性云服务器（Elastic Cloud Server，ECS）提供一种可弹性伸缩的云服务器，为用户提供安全、可靠、高性能的计算资源。QingTian系统是所有QingTian架构ECS实例的底层虚拟化平台，是华为云面向云数据中心构建的包括服务器定制、数据处理器、系统管理组件和专用固件的组合系统。

QingTian系统架构同时支持虚机、裸机和容器等多种形态及多元算力。基于QingTian系统，华为云构建了具有更强安全性、更强隔离性、更高性能和更低成本的基础设施云服务，并提供了可信计算、机密计算以及一系列面向多租户隔离和云服务隔离的安全特性。

在华为云，首要任务是保障客户工作负载的机密性（Confidentiality）、完整性（Integrity）和可用性（Availability），同时帮助客户满足其在数据安全和隐私保护方面的要求。华为云持续投资关键安全技术和工程最佳实践，致力于满足甚至超越客户对云上数据安全和隐私保护的极致要求。

本文档详细介绍了QingTian系统的安全设计，以及基于QingTian系统提供的面向租户的多维度隔离能力，帮助您评估ECS对于敏感工作负载的适用性。

- **QingTian系统简介**：介绍虚拟化技术，以及引入QingTian系统虚拟化后的架构变化。
- **QingTian威胁假设与安全方法**：介绍QingTian系统的威胁假设和安全设计方法。
- **QingTian系统组件**：介绍QingTian系统组件QingTian Cards（包含QingTian控制器和I/O功能卸载）和QingTian Hypervisor的一些关键安全设计。
- **QingTian机密计算**：介绍QingTian机密计算的设计理念，包括两个维度的隔离性设计和密码学证明。
- **物理隔离到逻辑隔离**：介绍以QingTian系统作为基石，如何强化从物理隔离到逻辑隔离的一系列安全隔离技术。
- **零特权运维**：介绍华为云生产系统的零特权运维理念以及关键安全系统保护实践。
- **案例：金融级客户数据安全上云**：从案例视角，面向金融级客户提供云上数据安全保护方案的一个设计参考。
- **结论**：总结QingTian系统功能和优势。

1.2 QingTian 系统简介

经典虚拟化系统

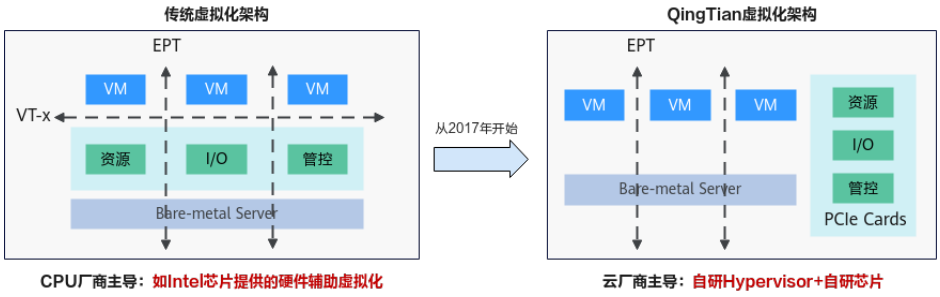
虚拟化支持在单个物理计算机系统上同时运行多个虚拟机操作系统。虚拟化系统通过硬件提供的辅助虚拟化能力，提供CPU虚拟化、内存虚拟化、IO虚拟化的功能，为客户的虚拟操作系统提供独立隔离的硬件使用空间。虚拟化技术能够将单个服务器资源分割给多个租户使用，每个租户虚拟机有独立隔离的定制化资源，从而实现对服务器的充分利用。

虚拟化系统的核心组件是Hypervisor，其职责包括对物理硬件资源的抽象与分配，以及对虚拟机（VM）的全生命周期管理和运行隔离，Hypervisor能实现同一物理机上不同虚拟机之间的资源隔离，避免虚拟机之间的数据窃取或恶意攻击，保证虚拟机的资源使用不受周边虚拟机的影响。终端用户使用虚拟机时，仅能访问属于自己虚拟机的资源（如硬件、软件和数据），不能访问其他虚拟机的资源，保证虚拟机隔离安全。

QingTian 虚拟化系统演进

QingTian系统架构是华为云推出的新一代软硬协同架构，核心实现了零资源预留、零算力损失、零业务抖动及强安全隔离等关键能力。华为云在2017年发布了基于QingTian系统的实例，一套QingTian架构同时支持虚机、裸机和容器等多种形态及多元算力。历经多年，QingTian系统重塑了华为云基础设施，当前已成为新一代实例的主流底层平台。

图 1-1 系统演进



QingTian系统主要由自研的专用QingTian Cards和自研的QingTian Hypervisor组成：

- QingTian Cards是由华为云设计的专有硬件加速设备，它提供整机系统控制和I/O虚拟化直通功能，且独立于前端主机系统运行，独立供电。

  QingTian Cards为整个系统提供基于硬件的信任根，确保整个系统的安全启动和可信度量，提供固件的防篡改保护，并提供基于硬件的IO加解密加速。
- QingTian Hypervisor是精简的轻量化虚拟机管理程序，它提供强大的资源隔离性和安全性，而且提供的虚机服务与裸金属服务器几乎无差别的超高性能。

专用QingTian Cards采用标准PCI-Express接口与主机系统CPU对接，并通过驱动把各种本地及网络资源模拟成主CPU的本地资源，让客户避免接触复杂的功能配置，更彻底地实现了云基础设施与客户应用之间的安全隔离保障。QingTian Cards还采用专用的ASIC硬件来处理存储、网络等虚拟化功能，这不仅提升了性能，还降低了成本。并且，采用QingTian架构可以大幅减少云基础设施底座与各种不同算力的适配工作，提升新功能迭代的速度。

1.3 QingTian 威胁假设与安全方法

威胁假设

为了给云上租户提供系统全栈的敏感工作负载运行隔离和数据保护能力，QingTian系统在安全设计上假设存在如下三类威胁模式：

- **威胁类型1：敌手通过控制VMM来攻击租户VM**

  这类威胁的典型模式包括：

  - 云上恶意租户通过购买ECS虚拟机实例，利用VMM零日漏洞或侧信道攻击模式实施VM逃逸攻击，进而控制VMM并攻击运行在同一硬件上的其它租户实例。
  - CSP内部人员因为部署、变更、调试、诊断等工作需要而使用合法凭证远程访问主机，并利用攻击者工具读取或篡改租户VM的敏感数据。

- **威胁类型2：敌手进入数据中心实施近端物理攻击**

  数据中心内部人员因为硬件部署、维护和修复原因而需要访问数据中心的物理设备，这可能产生的典型威胁模式包括：

  - 窃取硬盘后使用攻击者工具离线访问硬盘数据。
  - 窃听物理网络设备之间传输的所有流量数据。
  - 在服务器主板系统中预装、变更或注入恶意的固件。

- **威胁类型3：敌手通过控制Guest操作系统来攻击租户的敏感应用**

  这类威胁的典型模式包括：

  - 攻击者通过软件供应链方式植入不可信代码，利用Guest操作系统零日漏洞或错误配置实施提权攻击，获得Guest操作系统root权限后即可利用攻击者工具读取或篡改敏感应用程序及其数据。
  - 客户自己的内部人员因为部署、变更、调试、诊断等工作需要而使用合法凭证远程访问VM，并利用攻击者工具读取或篡改VM上运行的敏感应用程序及其数据。

安全方法

QingTian系统在安全设计上采用了如下原则和方法用以解决上述假设的三类威胁。

- **抵御恶意利用VMM**
  - 基于前后端分离式VMM架构方法，将VM管理和I/O功能虚拟化卸载到后端QingTian Cards，极大化隔离云系统管理与租户工作负载。
  - 基于最小TCB设计，提供前端QingTian Hypervisor，仅保留虚拟化运行最基本的代码，极大程度上消减VM逃逸风险。
  - 基于“ECS Control Plane --> QingTian Cards --> QingTian Hypervisor”的单向控制方法，仅允许单向发起连接初始化，逐级限制逃逸攻击的威胁半径，增强安全防御纵深。
  - 基于强制安全启动和可信度量方法，提供前后端系统固件、引导系统和Hypervisor的完整性保护和异常检测。
  - 基于零特权运维方法，提供运维操作API来替代传统的SSH远程登录访问服务器，极致裁剪操作系统并剔除协议栈和文件系统以及网络抓包工具和内存导出工具。

- **抵御近端物理攻击**
  - 基于数据加密方法，提供块存储加密和VPC流量加密，实现对租户VM相关的I/O数据在离开QingTian计算节点后的加密。
  - 基于硬件保护数据密钥方法，针对KMS硬件到QingTian Cards硬件，提供端到端的数据密钥安全分发。
  - 基于硬件身份认证、可信度量证明等方法，防止接入或挂载不可信硬件设备，避免启动被篡改的系统固件。

  此外，我们还将在新一代服务器中支持内存加密和总线数据加密，进一步提升系统安全基线。
- **抵御恶意利用Guest操作系统**
  - 基于可信计算方法，为租户虚拟机实例提供UEFI安全启动和QingTian TPM，支持标准的可信度量及远程证明方法，提供对Guest操作系统的完整性监控。
  - 基于将租户VM与云系统进行隔离的设计方法，为虚拟机实例提供QingTian Enclave特性，将虚拟机内的敏感工作负载与Guest操作系统进行隔离。

    租户的敏感工作负载仅在QingTian Enclave环境中运行，即使攻击者完全控制了Guest操作系统，也不影响Enclave运行环境的机密性和完整性。

1.4 QingTian 系统组件

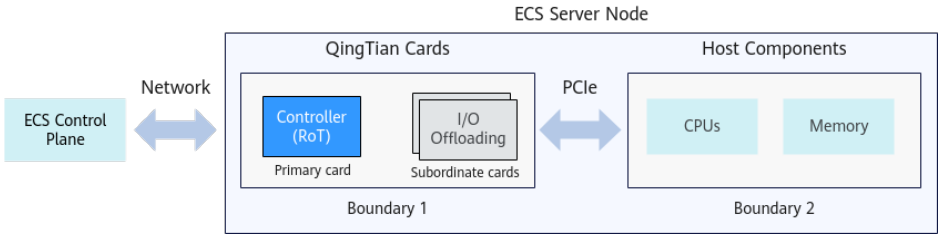
1.4.1 QingTian 系统组件概述

QingTian架构ECS服务器由QingTian Cards和主机系统组成：

- QingTian Cards是一组专用硬件功能组件，它独立于主机系统运行。
- 主机系统主要包含主机CPU和内存，运行客户的ECS VM实例或裸机实例。

QingTian Cards和主机系统是基于PCIe总线连接，分别隶属于两个完全隔离的系统安全域。

图 1-2 QingTian 系统组件



1.4.2 QingTian Cards

在逻辑上，QingTian Cards由一个主卡和多个从卡组成。

- 主卡：也称为QingTian控制器，负责管理服务器系统的所有其它组件及固件。
- 从卡：也称I/O功能卸载卡，提供专用的网络加速、存储加速、管控面加速及加密卸载等功能。

QingTian Cards包含了ECS服务管理计算节点所需要的所有控制接口，这些控制接口用于预置和管理主机CPU、内存和存储资源。对于ECS服务控制面来说，中心节点只需要

对接QingTian Cards，不需对接到服务器。服务器不包含存储和网络，来自ECS服务控制面的所有的虚拟机生命周期管理的命令，都直接下发到QingTian Cards，由QingTian Cards单向地操作前端服务器，比如创建虚拟机，关闭虚拟机，设备热插拔，虚拟机热迁移等。

QingTian Cards还提供服务器所有与外部交互的I/O接口，包括VPC网络接口、EVS块存储接口。对于服务器来说，它与外部世界交互的所有组件（无论是逻辑入站还是出站）都通过QingTian Cards来完成。QingTian Cards以PCIe设备形式连接到服务器上，可独立供电。卡上封装了华为自研的SPU芯片，用于固件启动和定制的极简OS运行。QingTian Cards支持卡上OS和关键虚拟化组件的热升级，并且跟主机服务器上的固件和系统组件升级相互独立，卡上系统的更新对客户业务几乎无感知，并且也不会影响任何原有的安全防护功能。

QingTian 控制器

QingTian系统支持基于UEFI Secure Boot标准的安全启动。服务器加电后，QingTian控制器首先执行安全启动，此时的主机系统处于等待状态。QingTian控制器中系统级芯片（SoC）的安全启动过程如下：

1. 启动只读存储器（boot ROM）。
2. 验证存储在QingTian控制器所连接闪存中的初期启动阶段固件的签名完整性，完成QingTian控制器自身的安全启动。
3. 验证所连接闪存中的QingTian Hypervisor镜像签名完整性，实现扩展信任链到前端主机系统。
   - 如果镜像签名验证失败，则上报启动异常事件并停止继续启动
   - 如果镜像签名验证通过，则通知主机系统继续执行安全启动。

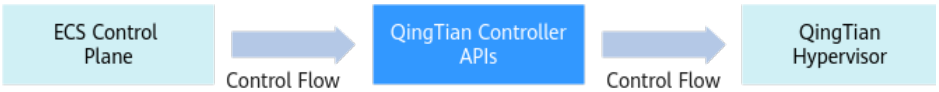
如果主机系统的安全启动失败，则上报启动异常事件。如发现启动异常，该节点会从服务节点中被摘除，因此不会运行客户的工作负载。

QingTian控制器也是物理服务器与云服务控制平面之间隔离的“安全网关”。云服务控制平面（包括ECS/BMS、EVS、VPC）在逻辑上独立且采用微服务架构，QingTian控制器将其统一抽象为“ECS Control Plane”进行交互。在交互模式上，遵循“ECS Control Plane --> QingTian Controller --> QingTian Hypervisor”的单向控制方法，仅允许单向发起连接初始化，所有反方向的连接初始化都被视为异常。

作为唯一通道，QingTian控制器将物理服务器与外部控制平面进行隔离，所有进出流量必须经由QingTian控制器进行安全转发。

- QingTian控制器向ECS控制平面提供基于mTLS的双向认证通信链路，确保数据传输链路的端到端加密。
- QingTian控制器API还提供基于API上下文属性的条件访问控制，来限制每个控制平面组件仅能调用其业务必需的最小API集合。同时，系统全量记录所有API操作日志（包括源网络上下文、身份上下文、调用参数、时间戳等信息），并支持实时的API异常调用检测。
- QingTian控制器通过专用网络与ECS控制平面通信，控制面进出流量与租户流量（如EVS存储数据流量、VPC网络流量）完全隔离。

图 1-3 QingTian 控制器交互模式



I/O 功能卸载

QingTian系统具备专有的I/O卸载加速硬件。这些卸载加速硬件与主控制器采用相同的系统级芯片（SoC）和基础固件架构，按不同功能需求，支持网络以及存储等硬件卸载加速，比如VPC卸载加速、EVS块存储卸载加速。这些卸载加速硬件通过集成于SoC中的硬件加密卸载引擎和安全密钥存储，为网络及存储提供数据加密功能及加速。

说明

华为云自研VPC加密：面向通用场景的标准安全协议IPsec、TLS不适用于大规模、高性能云数据中心的通信加密，华为云根据自身业务安全需求，推出了云网络CAE加密算法，用于满足华为云网络的多种场景下的加密传输要求，例如VPC内的用户虚机间加密传输、分布式云跨站点加密传输等。华为云支持在所有ECS实例之间提供安全和加密的连接，在某些实例支持使用QingTian专用VPC卸载卡实现实例之间的额外的传输流量加密。CAE协议默认使用AES-256-GCM算法自动透明加密实例之间的传输流量，加密协议在设计上支持匿名性(Anonymity)、抗重放(Anti-Replay)、前向安全(Forward-Secrecy)和后量子安全(Post-Quantum)。

专用的I/O卸载卡提供基于端到端加密的数据密钥导入和加解密算法的硬件加速功能，支持AES等标准密码算法以及GCM/XTS加密模式。用于EVS、VPC网络的加密密钥仅以明文形式存在于QingTian Cards内部的硬件密钥保护子系统中，华为云运维人员以及主机系统上运行的任何客户代码都无法访问它们。为了避免密钥分发系统可能存在的单点安全失效问题，控制面系统的多个密钥管理组件会独立实现多个密钥材料的安全分发。数据面无需执行密钥协商过程，而是在运行时基于控制面下发的多个密钥材料进行派生得到数据密钥，并实现密钥的小时级自动轮转。这一密钥分发机制更适用于云计算SDN架构，其能节省大量的密钥协商过程中的性能消耗，可以支持更大规模和范围内的通信加密。

当系统运行在QingTian Hypervisor模式下，QingTian Cards提供的I/O设备会通过SR-IOV（单根输入/输出虚拟化）技术细分为多个VF（虚拟功能），同时支持I/O设备直通虚拟机。这些VF可直接分配给VM，使VM获得对硬件接口（如网卡、存储控制器）的直接访问权限。在数据传输路径上，客户业务数据（如处理、存储或托管的内容）直接在客户ECS实例与QingTian Cards提供的虚拟化I/O设备间传输，绕过Hypervisor层实现硬件级数据直通。基于攻击面最小化原则，该方案使得I/O路径仅涉及VM、VF硬件及物理设备，这最大限度地减少了I/O路径中对软件和硬件的依赖，进而实现更高的安全性以及接近裸机的性能。

1.4.3 QingTian Hypervisor

QingTian Hypervisor通过轻量化重构设计、最小攻击面设计、防篡改设计和热升级技术设计，为租户ECS实例提供极致的隔离性和安全性保证。

轻量化设计

QingTian Hypervisor不同于传统的Type-1 Hypervisor，它在设计之初就对软件全栈进行了极致的轻量化重构设计：

- 全卸载架构：将传统管理面和I/O数据面全卸载至QingTian Cards，QingTian Hypervisor只保留基本的虚拟化和设备直通能力，服务器资源100%呈现给租户虚拟机。QingTian Cards管理面通过vsock安全通道对QingTian Hypervisor运行的虚拟机进行生命周期管理。所有虚拟磁盘与虚拟网卡通过QingTian Cards呈现为标准的virtio-PCI设备，在保证性能的同时，支持灵活的热插拔与热迁移。
- Huawei Cloud EulerOS 2.0：采用自研轻量级、无状态虚拟化基础OS，彻底移除与虚拟化无关内核模块和软件包，仅保留Hypervisor运行所必需的组件和模块。该系统体积小，易于传输，并支持内核漏洞的快速修复。

- VRAM：采用自研Pageless轻量级内存管理系统，摒弃传统单一的内存分页管理机制，虚拟机兼容传统内存特性的同时，内存管理开销降低数十倍。

最小化攻击面

相比传统Hypervisor，极致轻量化后的QingTian Hypervisor同时也会考虑各种外部攻击源对虚拟化数据面的影响。QingTian Hypervisor通过结合使用多种技术手段来实现最小化攻击面：

- 极小TCB：软件代码极致裁剪，仅保留虚拟化运行最基本的运行代码。
- 无网络：网络功能全裁剪，通过vsock唯一安全通道与QingTian Cards控制系统交互，进一步降低管理面攻击风险。
- 无存储：服务器无本地盘设计，无磁盘文件系统，无配置文件，日志和监控通过API定期记录至云端，无外部可编辑或修改的状态数据。
- 强绑核：虚拟机运行CPU固定，QingTian Hypervisor无需调度CPU，避免上下文切换带来开销的同时，消减侧信道攻击的风险。
- 强隔离：结合硬件辅助虚拟化和自研VRAM内存管理机制，确保虚拟机之间内存、I/O无法越界访问。

防篡改设计

QingTian Hypervisor软件包轻量化裁剪后，与安全启动过程联动，实现主机启动过程的可信校验。QingTian控制器会使用附有关联数据的认证加密算法（Authenticated Encryption with Associated Data，AEAD）来保护启动过程中敏感配置数据的机密性和完整性，确保仅当加解密上下文符合预期的可信环境中才会正确解密配置数据。在QingTian Hypervisor运行过程中，内存文件系统配置为只读，同时开启运行时可信审计，避免虚拟机逃逸或外部软件篡改。QingTian Hypervisor软件包升级同样经过CRC与证书等多重校验，确保软件包在运输过程中无篡改。

系统热升级

传统Hypervisor系统软件升级需要进行停机部署或将业务迁移后再进行升级部署，会引发客户业务中断感知风险，并且升级部署效率低。QingTian Hypervisor会定期进行快速更新，为应对不同的升级场景诉求，QingTian Hypervisor提供全面的安全热升级功能，支持函数级热补丁、组件级热替换以及Hypervisor整系统的原地热升级。在整个升级过程中，客户业务基本无感知。受益于QingTian Hypervisor的原地热升级的关键能力，无需进行迁移业务和主机重启的耗时操作，就可以在集群内实现快速大批量并行升级，确保软件版本发布之后可以迅速上线。即使在升级过程中，系统仍保持完整安全策略和防御能力。

1.5 QingTian 机密计算

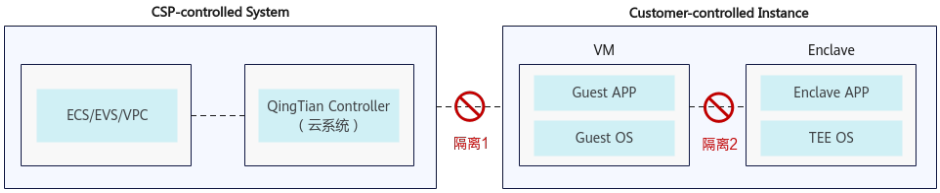
1.5.1 QingTian 机密计算概述

QingTian机密计算的设计目标是使用专用硬件和相关固件作为可信根来保护客户应用代码和处理过程中的数据免受外部访问：

- 机密性保护：确保客户数据/代码不会被CSP内部人员、云系统、客户自身的内部人员或VM管理员访问。

- 完整性保护：确保客户数据/代码不会被CSP内部人员、云系统、客户自己的内部人员或VM管理员篡改。

图 1-4 QingTian 机密计算



为此，QingTian机密计算的安全隔离设计考虑如下两个维度：

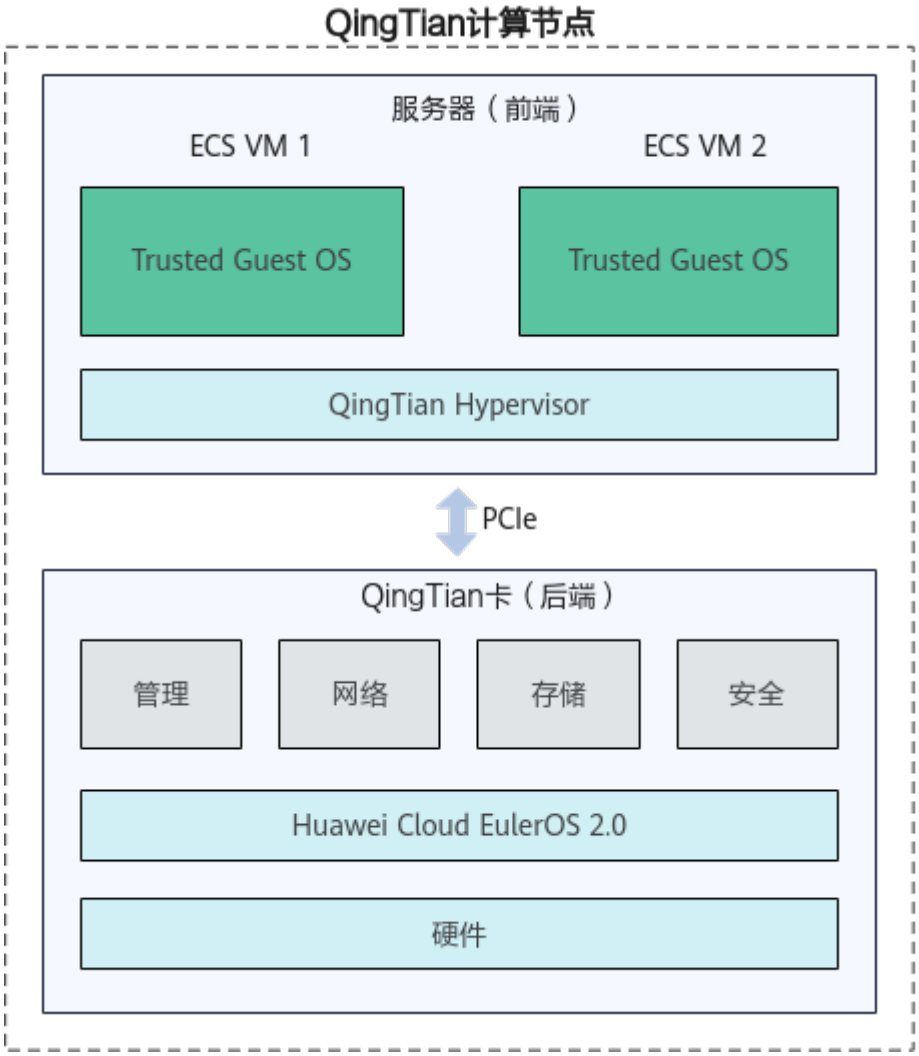
- 隔离维度1：将“客户代码和数据”与“云厂商内部人员和云系统软件”隔离。
- 隔离维度2：将“客户代码和数据”与“客户内部人员和低可信Guest OS”隔离。

1.5.2 隔离维度 1

QingTian系统的初始设计目标之一就是要支持将客户工作负载与CSP云基础设施之间进行安全隔离，这包括QingTian裸机实例和QingTian虚拟机实例。

- 对于QingTian裸机实例，QingTian Cards与主机系统完全隔离，由于主机系统没有运行QingTian Hypervisor，客户完全独占访问底层主板系统并能够使用相关的CPU硬件特性（如ARM TrustZone）。
- 对于QingTian虚拟机实例，我们基于QingTian Hypervisor提供了轻量化重构设计、最小攻击面设计、防篡改设计和热升级技术设计，组合使用这些技术，可以提供与裸机实例类似的隔离强度。

图 1-5 隔离维度 1



QingTian系统在这一隔离维度上采用如下方法来实现QingTian虚拟机实例的安全增强：

- 强隔离：QingTian系统是一种前后端分离式VMM架构，前端和后端系统是基于PCIe总线的物理隔离。前端Hypervisor基于硬件辅助虚拟化和自研VRAM内存管理机制来确保虚拟机之间内存和I/O访问隔离，QingTian Cards通过SR-IOV支持VM实例直通访问硬件设备。并且使用强绑核来固定虚拟机的运行CPU，QingTian Hypervisor无需调度CPU，避免上下文切换带来的侧信道攻击风险。
- 防逃逸：基于最小TCB的设计理念，QingTian Hypervisor代码极致裁剪，仅保留虚拟化运行所需的最基本代码，无网络协议栈，无本地盘，无配置文件，无SSH管理工具等。相比传统虚拟化管理系统，QingTian Hypervisor代码量不足其1%，极大程度上消减了VM逃逸风险。
- 防篡改：QingTian系统使用强制的安全启动和可信度量。QingTian控制器首先执行安全启动，确保启动环境符合预期后再验证QingTian Hypervisor镜像文件完整性并引导主机系统启动QingTian Hypervisor。
- 保护密钥：QingTian Cards内置独立的硬件安全模块，基于硬件保护的身份认证来建立与ECS控制面的可信接入，避免软件凭证泄露导致的节点身份伪造。

QingTian控制器使用硬件安全模块来保护Volume加密、VPC加密所需的密钥材料，在硬件环境中实现数据密钥派生，确保数据密钥不出硬件。

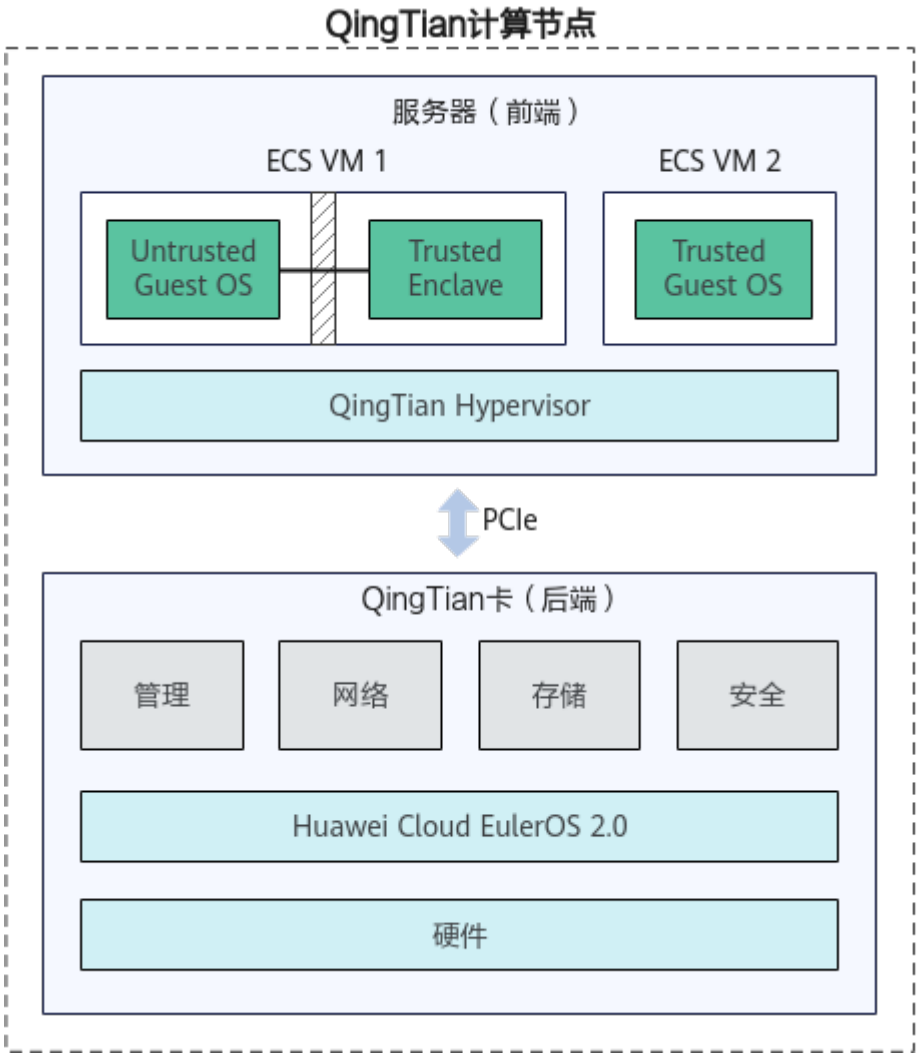
- 无人接触生产：QingTian Hypervisor不提供任何可用于远程登录的机制。云服务运维人员通常只能使用运维API来进行远程诊断，没有内部人员可以获得系统特权去访问客户实例的内存数据。

1.5.3 隔离维度 2

在云基础设施平台上，提供虚拟机实例Guest OS的启动完整性保护已经成为新的安全基线。当前，ECS虚拟机实例已提供UEFI安全启动（Secure Boot）和QingTian TPM特性，支持客户实现满足TCG标准的可信启动和远程证明能力。QingTian TPM是由QingTian系统提供的符合TPM 2.0规范的一种虚拟设备，操作系统一般会基于TPM来实现磁盘加密（如Windows BitLocker）、数据防篡改（如Linux DM-Verity）等安全特性。

然而，通用客户虚拟机操作系统（如Rich OS）一般拥有较大的TCB，这往往导致存在较大的攻击面，尤其是Guest OS运行时完整性保护仍然存在诸多挑战。那么，在这一隔离维度上，我们参考隔离维度1中将租户VM与云系统进行隔离的设计方法，提供QingTian Enclave来运行租户的敏感应用。它将Guest OS划分在QingTian Enclave的信任边界之外，将敏感应用的运行环境与Guest OS运行环境进行完全隔离，确保Guest OS存在的安全威胁并不会影响Enclave环境中的应用和数据安全。

图 1-6 隔离维度 2



QingTian Enclave是在ECS实例内部由用户启动的一个与父实例完全隔离的VM运行环境，它通过唯一的vsock安全通道连接到父实例。基于父实例Guest OS不可信假设，QingTian Enclave在这一隔离维度上采用如下方法实现安全增强：

- 强隔离：QingTian Enclave与客户父ECS主实例之间基于硬件辅助虚拟化和自研VRAM内存管理机制来确保虚拟机之间的隔离，Enclave与父实例之间没有共享的物理内存和CPU Core，仅通过唯一的受Hypervisor保护的本地vsock安全通道进行连接。即使主实例Guest OS存在安全缺陷，或者超级管理员权限被攻破，控制了主实例Guest OS的攻击者仍然无法访问Enclave环境中的代码和数据。
- 最小攻击面：QingTian Enclave不支持挂载网卡，不提供网络接口，不提供持久化存储，也不支持SSH交互式访问。QingTian Enclave OS 默认使用一个华为云自研的经过极致裁剪的安全OS，当然客户也可以定制自己的Enclave OS。
- 防篡改：QingTian Enclave启动时，QingTian Hypervisor会验证Enclave镜像的数字签名，并度量Enclave镜像文件和数字签名公钥证书，度量结果会保存到QTSM（QingTian Security Module）。QTSM提供类似TPM的可信度量和远程证明特性，与TPM的主要差别是QTSM基于云计算ECS服务场景重新定义了可信度量属性和Attestation安全协议。

- 保护密钥：为了保护QTSM的关键密钥和运行时安全，QTSM运行在QingTian Cards提供的隔离计算环境中，基于TRNG硬件引擎产生随机的Attestation密钥对，然后向QingTian Attestation PKI服务申请Attestation公钥证书。QingTian Attestation PKI服务在通过硬件增强的身份认证之后，为QTSM颁发Attestation公钥证书。QTSM还支持Attestation密钥对的小时级轮转，这进一步消减了密钥泄露的风险。

QingTian Enclave支持远程证明协议。Enclave应用与外部依赖方建立信任时，可以通过Attestation协议向依赖方提供Enclave身份和运行环境度量的密码学证明。华为云KMS、IAM服务内置了对QingTian Enclave Attestation的支持。Enclave应用开发者可以使用开源Enclave SDK访问KMS API来获取数据加解密密钥或安全随机数并保证端到端的安全。IAM管理员可以通过预设的IAM授权策略或护栏策略来对KMS API施加基于Attestation的条件访问控制。

此外，在易用性和应用兼容性方面，QingTian Enclave也是一个对开发者友好的平台。开发者无需具备CPU微架构专业知识和高级密码学知识就能轻松开发QingTian Enclave应用。当前QingTian Enclave已支持x86和ARM架构，开发者可以使用任何熟悉的开发语言框架，并基于容器镜像直接构建QingTian Enclave镜像。

QingTian Enclave使能客户在ECS VM环境内部创建出一个强化且高度隔离的计算环境，以满足客户将自身系统组件按不同信任等级进行隔离。QingTian Enclave特性自上线以来已获得众多云上客户的青睐，客户基于QingTian Enclave构建的生产应用有vHSM加密机、Vault凭证管理、MPC数字钱包等。针对云原生机密容器解决方案，我们还支持在Kubernetes中配置QingTian Enclave设备插件(Device Plugin)，以支持客户Pod和容器能够访问QingTian Enclave设备驱动，该设备插件适用于CCE或客户自管理的Kubernetes节点。此外，华为云还提供了丰富的QingTian Enclave开源工具（eg, qproxy）和安全解决方案，帮助更多客户实现无需改造应用代码和构建系统，即可以平滑迁移至QingTian Enclave环境。

说明

QingTian Enclave适用场景：QingTian Enclave可以为应用程序提供一个满足最小攻击面的极致隔离运行环境，这个环境不允许弹性网卡挂载和存储卷挂载，不支持网络协议栈和持久化存储，它只能通过连接到主实例的vsock安全通道并借助主实例的网络代理才能访问外部网络。即使主实例Guest OS被彻底攻破，也不会影响Enclave环境的应用程序代码和数据安全。如果用户需要在隔离环境中挂载弹性网卡或存储卷，或需要访问GPU设备，那么QingTian Enclave并不适用，而推荐使用支持QingTian TPM的ECS实例。

1.5.4 密码学证明

QingTian Enclave 证明

QingTian Enclave提供启动度量和远程证明能力。QingTian Enclave的度量值由通过标准的可信度量运算操作 (ExtendPCR) 得到的一组哈希值组成，这组哈希值保存在QTSM (QingTian Security Module) 的平台配置寄存器PCR中。QTSM可以支持最多32个PCR度量属性，PCR [16~31]可以由Enclave应用程序进行自定义，PCR[0~15]由QingTian系统预留，当前已支持的度量属性包括PCR0（QingTian Enclave镜像文件）、PCR3（IAM Agency URN）、PCR4（ECS Instance ID）、PCR8（QingTian Enclave镜像文件签名证书）。

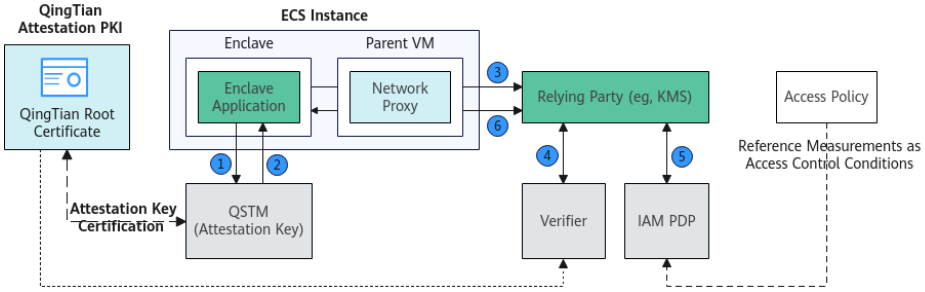
Enclave应用程序可通过QTSM获取当前Enclave环境的一个可信证明文档 (Attestation Document)。证明文档包括PCR度量属性列表、QingTian PKI证书链、密码算法声明以及用户自定义参数。QingTian Enclave证明文档支持的用户自定义参数非常丰富，包括pubkey (由QTSM签署的用户自定义公钥)，nonce (避免重放攻击的一次性数据)和 user_data (任意自定义数据)，它可以支持Enclave应用程序与外部实体之间运行多

种自定义安全协议（eg，安全密钥协商、端到端加密）以实现复杂的应用安全解决方案。

华为云KMS服务、IAM服务内置了对QingTian Enclave Attestation协议的支持。租户IAM管理员可以通过设置条件授权策略来实现特定的安全控制目标，比如仅允许指定的Enclave应用程序才能调用指定的KMS API操作（比如生成随机数、加密、解密等）。下图展示了Enclave应用如何使用包含自定义pubkey参数的证明文档去访问KMS Decrypt API以实现密文数据解密的操作流程：

1. Enclave App首先随机产生一个RSA密钥对(prikey, pubkey)，使用pubkey作为参数调用QTSM API产生证明文档。
2. QTSM计算AttestationDoc（包含pubkey）并返回给Enclave应用。
3. Enclave App携带AttestationDoc和密文数据Blob，调用KMS Decrypt API。
4. KMS使用Verifier SDK来验证AttestationDoc有效性。
5. KMS将Verifier验证结果提供给IAM PDP（Policy Decision Point）进行访问控制决策。
6. KMS在访问控制策略检查通过后解密Blob，并使用AttestationDoc所携带的pubkey对解密结果进行重新加密封装后返回；Enclave App收到响应后，使用步骤1中产生的prikey解封装后得到明文。

图 1-7 密文数据解密过程



QingTian TPM 证明

用户在创建ECS实例时可选择配置UEFI安全启动模式并使能QingTian-TPM。QingTian-TPM 是QingTian系统为ECS实例提供的一个虚拟设备，并遵循TPM 2.0技术规范。QingTian-TPM提供度量启动和远程证明，用户可以从QingTian-TPM获取签名的PCR值，并使用它们向远程实体证明ECS实例启动时的完整性。QingTian-TPM 还可以产生密钥并将其用于加密或签名，QingTian-TPM产生的密钥可以用于向依赖方提供设备身份证明。

ECS 实例身份证明

- **使用实例身份文档**

  用户启动的每个ECS实例都有一个实例身份文档（Instance Identity Document），该文档提供有关实例本身的元数据信息，这些信息包括实例规格、实例ID、镜像ID、归属账号ID、私网IP地址、创建时间等。用户可以使用实例身份文档来验证实例相关的属性。运行在ECS实例中的应用程序可通过实例元数据服务IMDS (Instance Meta Data Service) 获取实例的实例身份文档以及针对实例身份文档的一个数字签名。当应用程序需要将实例身份文档发送给一个远程实体（依赖方）验证时，通常需要提供实例身份文档及其数字签名。从IMDS获取实例

身份文档的数字签名时，用户可以提供自定义的audience参数（eg，通常为仅使用一次的挑战值）来避免重放攻击。

实例身份文档及数字签名可看作是ECS服务为每个ECS实例提供的一个默认的“出生证”。当实例中的应用程序需要与远程实体进行交互时，该“出生证”可用于实例的初始身份证明。有了“出生证”之后，基于“可传递信任”安全原则，应用程序可使用该初始身份来获取应用相关的访问凭证，从而可以有效解决身份安全问题（eg, 在应用程序配置文件中硬编码静态凭证问题）。

- **使用实例IAM委托**

  用户在创建ECS实例时可选择配置一个IAM委托。实例IAM委托（IAM Agency for Instance）是IAM管理员创建的一个虚拟身份，在此场景中它用于代表用户的ECS实例访问云服务资源时所使用的IAM身份。IAM委托的一个安全优势是没有静态凭证，所以能有效消减静态凭证（或长期凭证）的泄露风险。运行在ECS实例中的应用程序可通过实例元数据服务IMDS (Instance Meta Data Service) 获取实例IAM委托的一个临时安全令牌，该安全令牌由IAM令牌服务STS(Security Token Service) 签发，它代表实例IAM委托的一个身份会话。实例IAM委托在获得IAM授权后，应用程序可以使用实例IAM委托的临时安全令牌去访问被授权的云服务资源（eg，OBS对象）。

  实例IAM委托可看作是租户IAM管理员为ECS实例提供的一个自定义“机器身份”，当实例中的应用程序需要访问被授权的华为云服务资源或API时，可以使用该“机器身份”的临时安全令牌直接访问，而不需要在应用程序代码或配置文件中硬编码静态凭证（如AK/SK），从而避免静态凭证泄露风险。

  说明

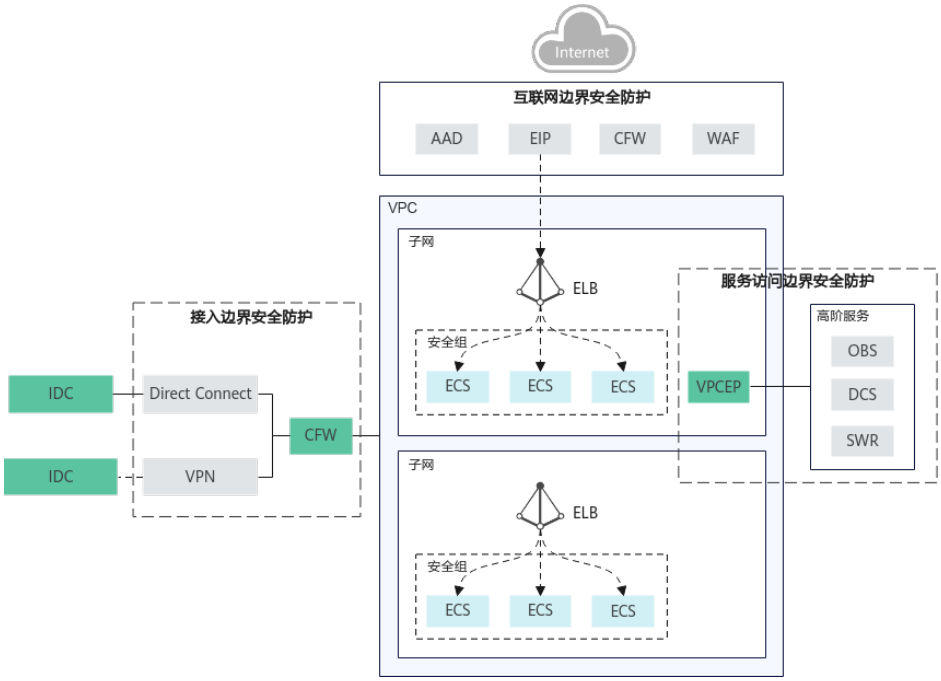
  推荐使用ECS IMDSv2协议访问实例元数据服务：相比IMDSv1而言，IMDSv2使用“PUT方法”和“动态令牌”来初始化IMDS会话，可以有效消减租户Web应用可能存在的SSRF漏洞风险，以及因为错误配置WAF、反向代理、三层防火墙或NAT所导致的潜在安全风险。使用IMDSv2可以显著增强租户ECS实例的纵深安全防御能力。

1.6 物理隔离到逻辑隔离

隔离技术是云平台安全的一个基石。在隔离性方面，华为云QingTian系统不仅为租户提供了运行环境的物理隔离，而且还作为一种可信计算基(TCB)，为租户提供了丰富的逻辑隔离能力，包括VPC网络隔离、多租户资源隔离和跨云服务访问隔离。

基于 VPC 的网络隔离

图 1-8 基于 VPC 的网络隔离



VPC是租户安全的一个基石，它为客户在云上的业务部署，提供了一个完全隔离的网络空间，构建了一个默认安全的网络环境。客户可以在做好安全控制的情况下，按需构建必要的网络通路。VPC和外界的通信通常有三大类网络连接模式（如图所示）：

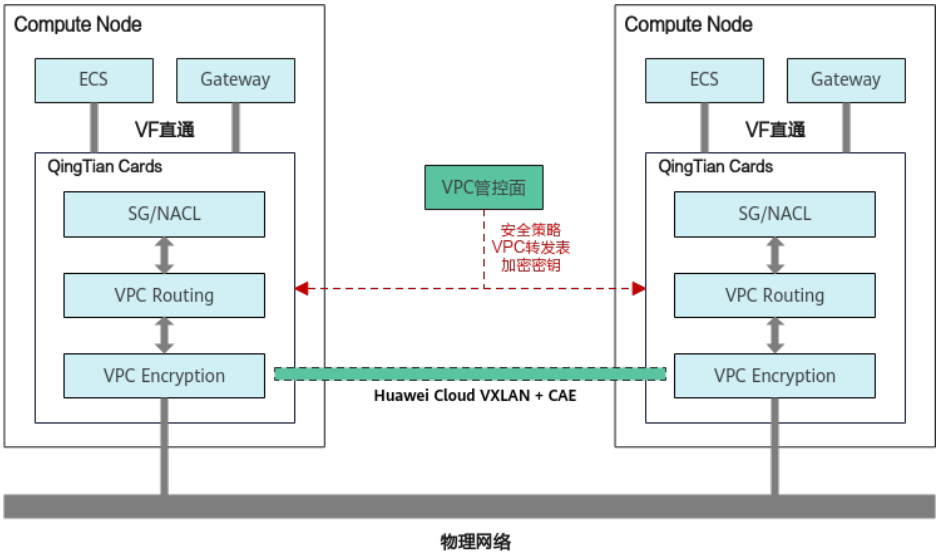
- 互联网访问：通过AAD、WAF、CFW等安全防护措施，保障通过EIP实现的互联网访问的安全性。
- 混合云接入：通过CFW等机制，保护通过专线、VPN等方式和客户线下机房互联的访问安全。
- 云服务访问：通过VPCEP实现访问云服务，并借助VPCEP Policy保障对云服务访问的安全控制。

VPC自身提供了Security Group和Network ACL两个基础网络安全访问控制能力，均为L4有状态网络安全能力：

- Security Group：以ENI（Elastic Network Interface）或者ENI集合为对象，配置进出ENI或ENI集合的访问策略。
- Network ACL：以Subnet为对象，配置出/入两个方向的访问策略，包括源目的IP、端口和协议等信息，并绑定指定的Subnet。

VPC还提供了网络加密能力。对于开启了加密的租户VPC，在此VPC内的计算资源、网关之间的互访流量，就会使用加密报文传输，确保客户流量对于云提供商而言是全量加密的，无法被破解侦听。

图 1-9 VPC 网络加密能力



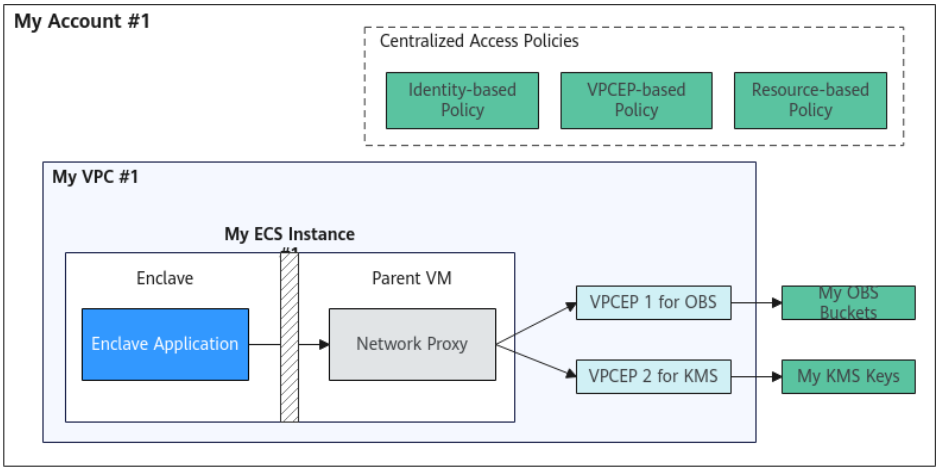
VPC提供的网络隔离、流量加密、以及基于Security Group和Network ACL的网络访问控制能力，都是通过QingTian硬件系统来实现的。VPC管控面将网络子系统所需要的表项下发到QingTian Cards，QingTian硬件通过VF直通实现ENI网卡的虚拟化，通过与计算资源（ECS、BMS、CCI等）相连来实现VPC内的转发。

- 安全访问控制模块：为实现Security Group和Network ACL访问控制，QingTian硬件通过报文所属的VF，找出其对应的ENI和Subnet，进而找到对应的Security Group和Network ACL安全策略，执行策略评估后决策是否转发，并形成状态防火墙所需的会话表项，确保后续报文正确通过。
- VPC路由模块：为实现报文的VPC隔离转发功能，QingTian硬件会根据报文所属的ENI和Subnet，查找客户VPC专属的路由表项，并做VxLAN隧道封装并发送。目的端QingTian硬件，也会根据VxLAN封装中的信息，找到报文所属的VPC专属路由表并转发。整个转发过程，都是通过查找VPC专属的路由表，实现网络转发隔离。
- VPC加密模块：为实现VPC流量加密，QingTian硬件会根据报文的VPC属性，找到VPC专属的加密密钥，在VxLAN隧道上增加加密报文头，实现对于客户全部报文的加密，包括客户报文的MAC、IP等转发信息，以及VxLAN隧道中有关报文所属VPC的附加信息。由于加密密钥是在租户VPC所涵盖的计算节点中共享的，因此目的QingTian硬件能根据密钥ID找到密钥并解密后，继续后续转发流程。

云服务访问的多租户资源隔离

在租户VPC中，部署在Enclave（或VM）上的客户应用可能会依赖多个云服务的API调用，比如依赖OBS或KMS服务。由于这些被依赖的云服务是部署在租户VPC之外，这就需要打破VPC网络隔离边界让客户应用能够访问云服务API。针对这种场景，华为云提供VPC终端节点服务来满足这一场景。VPC终端节点通过单向访问、Endpoint策略来控制这一访问路径上的攻击面。

图 1-10 多租户资源隔离



云服务API默认提供多租户资源访问控制隔离能力，这种访问控制隔离是基于IAM (Identity and Access Management) 访问控制体系进行构建的。华为云IAM服务为租户提供集中的身份与访问控制管理，提供统一的访问控制策略语言，并为所有云服务API提供一致的访问控制决策。IAM访问控制决策引擎（Policy Decision Point，PDP）支持多种类型的访问控制策略，这些策略类型包括基于VPCEP的策略、基于IAM身份的策略和基于云服务资源的策略。IAM访问控制策略支持丰富的访问控制条件属性，目前已支持50+的全局条件属性和云服务相关的500+条件属性。这些条件属性主要包括身份主体属性、会话主体属性、运行环境属性、网络相关属性、API上下文相关属性和目标资源相关属性。租户可以在自定义的IAM策略设计中组合使用合适的条件属性集，灵活实现满足自身业务所需的安全控制目标或业务合规要求。

IAM PDP引擎依赖的运行环境属性和网络相关属性完全是由QingTian系统来提供正确性和完整性保证。QingTian系统会通过IAM Context Provider机制在IAM服务中注册元数据，内容包括上下文的验证公钥和上下文断言Schema。QingTian系统会在相关的API访问链路中注入带数字签名的上下文断言(Context Assertions)，IAM PDP引擎会验证这些上下文的完整性，并基于这些可信的上下文断言来执行API请求相关的访问控制策略评估逻辑。

跨云服务访问的多租户资源隔离

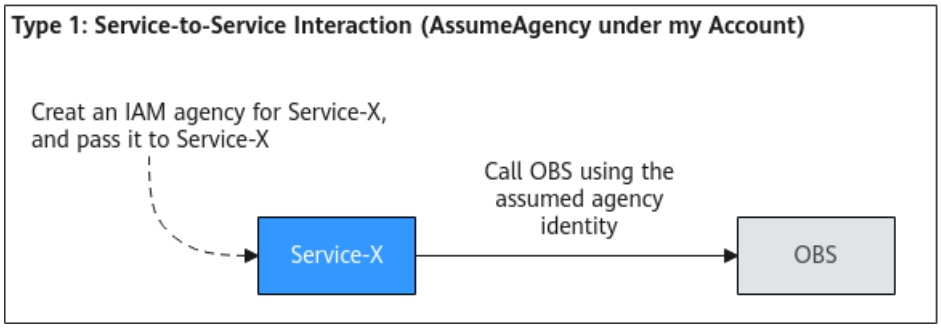
如果您的租户账号订阅了多个云服务，而且这多个云服务之间可能会涉及跨服务的资源访问。由于跨云服务资源访问通常会遇到Confused Deputy安全问题，如果云服务的访问隔离设计不当，很容易导致您的云服务资源会被其它租户越权访问。

华为云从访问控制技术协议设计层面来解决Confused Deputy问题。在协议设计上，一个租户账号下订阅的云服务的身份主体（Service Principal）会默认被限制在该租户的账号域之内，并且同一账号域内的不同云服务之间默认完全隔离，所有的跨云服务访问需要租户的显式授权。

华为云IAM提供AssumeAgency 和 Impersonation两种安全协议，面向两种不同的跨云服务访问场景，实现租户账号域内的跨云服务授权访问。

- **协议1：AssumeAgency协议（委托代持）**

图 1-11 委托代持

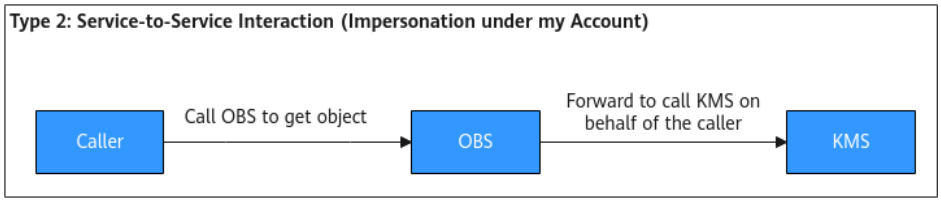


AssumeAgency协议的典型场景是用户离线后的云服务作业需要授权访问下游的云服务资源。管理员创建一个IAM云服务委托 (Agency)，在信任策略中指定 " Service-X" 作为受信任的主体；然后给此委托授予合适的权限，并将此委托配置到Service-X。

IAM Agency的信任策略中的受信任主体 " Service-X" 默认表示我的账号域（或组织域）下的Service-X。也就是说，任何其它账号所订阅的Service-X并没有获得信任，其它账号域下的Service-X并没有获得代持该委托的权限。通过引入账号域（或组织域）的设计，我们可以在协议层面解决跨云服务访问的Confused Deputy问题，提供默认的多租户安全隔离。

- **协议2：Impersonation协议（身份模拟）**

图 1-12 身份模拟



Impersonation协议的典型场景是用户在线时的云服务请求处理逻辑需要访问下游的云服务资源，比如“User -> OBS -> KMS”的访问。管理员无需给云服务OBS额外授权，该协议可以支持OBS模拟当前请求者身份和权限去访问下游云服务KMS。

我们结合一个实际例子来说明该协议的安全设计。比如，User调用OBS GetObject API，并且Object数据使用了租户KMS密钥进行加密。由于当前租户下的OBS服务主体并没有被授权访问租户KMS密钥，那么OBS需要使用Impersonation协议来模拟当前用户去调用KMS API。

具体设计上，OBS会提供当前请求者的“API RequestProof”去访问STS（Security Token Service）申请一个转发访问令牌，然后使用该令牌来构造KMS API的访问请求。“API RequestProof”为Impersonation协议提供了安全保证。“API RequestProof”包含有API名称、API签名及过期时间信息，STS会校验此API是否有关联的Impersonation使用许可、API签名是否有效，然后决定是否发放相应的转发访问令牌。此外，OBS获得的转发访问令牌的权限是 “当前用户已获得的授权” 与 “此API关联的Impersonation会话缩权策略（scope-down session policy）” 的一个交集。与一个API所关联的Impersonation会话缩权策略是基于最小授权原则进行设计的，它需要经过云安全团队、IAM团队和云服务团队的多方评审后才能被注册到生产环境。

1.7 零特权运维

在**QingTian威胁假设与安全方法**，我们假设云厂商内部人员也是一种潜在的攻击媒介，可能会通过逻辑访问方式或物理访问方式对租户数据安全造成潜在威胁。因此，QingTian系统引入“零特权运维”理念，通过技术最佳实践和运维安全管理相结合，最大化消除此类安全隐患。

- 零SSH权限：运维人员无法通过常规的远程登录方式获得对服务器的控制权，所有对服务器的运维操作均通过API方式进行，所有的运维管理API都有严格的身份认证、授权、记录和审计，这些API不支持为操作人员提供访问服务器上的客户数据。
- 零抓包工具：服务器节点的OS经过极致裁剪，去除了TCPDump等常用的抓包工具，避免租户的IO数据被监听或窃取。
- 零内存权限：通过QingTian自研的内存管理组件VRAM独立管理虚拟机的内存，不支持通过传统的virsh dump方式导出内存。

这些技术限制内置于QingTian系统本身，具有最高权限的系统管理员也无法绕过这些控制和保护。由于禁用了常规的登录访问功能，生产环境不支持就地调试。无法就地调试会给技术人员带来不便，但我们坚信这对我们的客户来说是更好的权衡。因此，我们必须在生产发布之前保持高标准的系统质量和测试。

云基础设施安全还依赖于多个关键系统的根密钥保护。根密钥保护需要应对各种威胁媒介，包括来自拥有最高权限的内部人员的潜在威胁。仅依赖单一硬件加密机的根密钥保护技术因为存在单点安全失效问题，不足以应对日益严峻的攻击挑战。QingTian系统采用以下方法和措施来实现对关键系统密钥的保护：

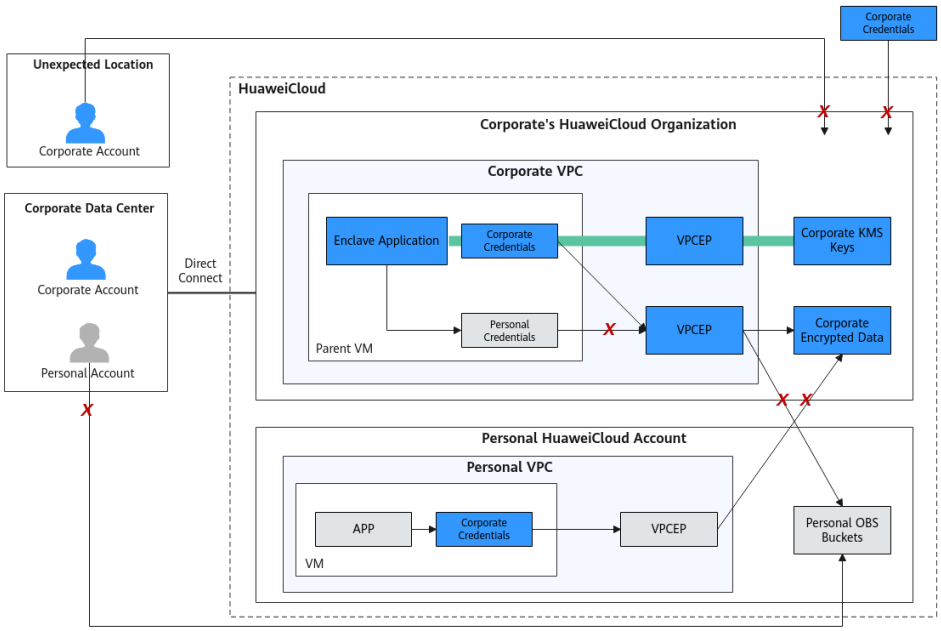
- 门限数字签名：部分关键系统采用门限数字签名算法对签名密钥进行拆分，并在拆分后将原始密钥彻底销毁。拆分后的N个密钥分片由多个独立节点分别持有，其中任意T个计算节点可以按照门限签名协议协作完成对一个消息的签名，而少于T个节点则无法进行签名。签名过程中自始至终不会出现完整密钥，且没有任意单点持有完整密钥。这种方法不仅提升了密钥管理的安全性，还提升了系统的可用性。
- 多重密钥材料：部分关键系统采用多重数字签名技术（依赖多个签名密钥）来实现防篡改。另有部分系统则基于多个独立的密钥材料合成数据加解密密钥。每个独立的签名密钥或密钥材料由安全硬件提供保护，避免攻破单一密钥所导致的系统性安全风险。
- 密钥不可导出：工作密钥使用硬件身份公钥加密后被导入QingTian Cards内置的硬件密钥保护模块中，不可以明文的方式再被导出硬件，仅能通过模块API以受限的认证和授权方式被使用。
- 密钥快速轮转：系统严格保证密钥的轮转周期与其使用频率呈反比，对于被高频使用的工作密钥（如终端实体证书密钥）实现小时级轮转。
- 租户级密钥隔离：系统为不同租户分配完全独立的随机密钥材料，并基于此进行租户级密钥派生。派生后的密钥仅对单租户有效，避免攻破单一密钥材料所导致的全局性安全影响。

密钥保护问题一直以来都是一个开放的挑战，我们持续将关注最新的密码学技术进展（如门限密码学技术），率先在云工程最佳实践中引入这些新技术来提升安全门槛，并刷新当前的工程安全最佳实践。

1.8 案例：金融级客户数据安全上云

金融客户对数据安全有非常严格的要求。基于华为云在金融领域客户上云安全解决方案中积累的最佳实践，我们提出了一种面向金融客户数据安全上云的参考框架。

图 1-13 金融客户数据安全上云



- **目标1：核心敏感数据仅在TEE机密边界内处理**

  云上所有的持久化数据默认加密，比如通过组织护栏策略强制执行OBS桶加密、EVS卷加密、RDS数据库加密等等。应用程序针对核心敏感数据使用一层额外的加密，数据密钥由客户控制的KMS主密钥保护，通过IAM条件访问控制策略确保数据密钥仅在预期的QingTian Enclave环境中才能被解密使用。华为云KMS支持QingTian Enclave Attestation协议集成，支持将数据密钥、随机数和解密结果使用端到端加密方式从KMS安全传送到Enclave环境，从而实现核心敏感数据仅在TEE环境中被解密和处理。

- **目标2：构建生产环境中的数据边界护栏**

  通过VPC网络配置来设置网络边界，阻止非预期的Internet出入流量、非预期的跨VPC之间的访问流量以及非预期的云服务访问流量。在网络边界控制的基础上，增加使用身份与访问控制方法构建组织的数据边界护栏：

  - 面向身份的数据边界护栏：使用SCP来定义组织账号内所有IAM身份的权限边界，以确保组织账号内的IAM身份凭证只能使用组织的VPC终端节点（禁止公网和其它访问路径），以及只能访问归属于组织账号的云资源。身份护栏构建完成后，即使出现IAM身份凭证泄露，攻击者无法使用身份凭证从Internet或从他人的VPC终端节点发起访问，从而可以消减凭证泄露的风险。
  - 面向VPC终端节点的数据边界护栏：使用VPC终端节点策略来设置权限边界，以确保经过VPC终端节点的云服务API请求仅来自组织账号内的IAM身份，且只能访问归属于组织账号的云资源。
  - 面向资源的数据边界护栏：使用资源授权策略来设置权限边界，以确保资源的所有API请求只能来自组织账号内的IAM身份，以及必须通过组织的VPC终端节点（禁止公网访问路径）。

- **目标3：安全身份接入与凭证防泄漏**
  - 基于标准身份联邦协议构建面向员工的身份联邦登录解决方案，禁止绕过企业本地登录系统来使用云账号。关于租户登录限制，实施对SSO登录和控制台访问操作的指定网络位置限制，以及使用企业本地安全网关来实施租户登录限制，从而达到限制员工从企业内部只能登录企业云账号，无法登录个人账号。
  - 构建应用身份联邦，支持租户应用使用SAML、OIDC协议实现外部令牌到华为云IAM令牌的安全交换。禁用所有IAM用户，全面使用IAM Agency来替代IAM用户，以彻底消除长期凭证（eg, AK/SK, 登录密码）泄露风险。强制使用ECS IMDSv2方式访问ECS实例身份签名和IAM委托身份令牌，使用SCP策略限制IAM令牌的身份边界护栏，消除IAM令牌泄露到VM或VPC之外导致的风险。

1.9 结论

本文从QingTian架构系统安全到租户安全，为客户提供了E2E的安全解决方案，保证客户的敏感业务以及敏感数据可以在安全的环境中运行以及如何避免关键敏感数据的泄露。

这些安全的关键能力依赖于QingTian架构的QingTian Cards、QingTian虚拟化、QingTian控制器的软硬协同，以及定制化硬件的安全防护。

目前，所有新的ECS实例类型都基于QingTian系统构建，为客户提供了本文中讨论的所有安全防护和优势，客户可以根据业务敏感程度选择最适合工作负载的实例和安全保障。

1.10 声明

本文档针对华为云QingTian架构的系统安全设计进行综合阐述：

- 仅提供安全设计信息参考。
- 仅限当前的华为云产品和服务，这些内容可能会在未通知客户的情况下发生变化。

本文档内容不构成提供任何形式的担保、声明或承诺。华为云对客户的责任和义务由华为云与客户之间签署法律协议约定。本文档不构成华为云与客户之间有法律效力的协议，也不构成对华为云与客户已经签署的协议的变更或修改。

