intel XEON

白皮书

第四代英特尔® 至强® 可扩展处理器
英特尔® TDX
云实例

英特尔® TDX 云上落地，助力阿里云第八代企业级 ECS 实例为企业云服务提供更优安全防护

阿里云

“阿里云从成立的第一天起，安全可信就是第一属性。阿里云一直致力于通过各种方式使阿里云对客户更透明，且用户数据的保护是其中不可分割的重要部分。除了严密的安全规约外，我们也在通过各种硬件安全技术来实现用户'可验证'的数据保护机制。第四代英特尔® 至强® 可扩展处理器在强劲的算力之外，其提供的英特尔® TDX 技术也有力地支持我们为客户提供了更便捷和更多样化的机密计算服务。”

刘煜堃
阿里云高级安全专家
阿里云安全团队

前言概述

作为新一代的数字基础设施，云计算服务正逐渐成为各行业实施数字化转型，实现业务再突破的重要引擎之一。而随着数据价值的不断突显与相关政策的持续出台，云服务的安全性也正受到越来越多客户的关注。作为全球领先的云服务提供商与先进机密计算服务的领跑者，阿里云正与英特尔展开合作，将全新第四代英特尔® 至强® 可扩展处理器引入其最新的第八代企业级 ECS 实例 g8i 中，以应对更为多样化的云服务模式需求。

英特尔全新发布的第四代至强® 可扩展处理器在为阿里云第八代企业级 ECS 实例提供强劲的算力支持之外，新处理器内置的英特尔® TDX 技术，也为阿里云向客户提供面向虚拟化实例的机密计算新方案提供了坚实的技术保障，助力客户在不改变现有应用程序的情况下，为其基础设施即服务 (Infrastructure as a Service, IaaS) 和平台即服务 (Platform as a Service, PaaS) 应用分别构建基于硬件设备的可信执行环境 (Trusted Execution Environment,TEE)，如机密虚拟机或机密容器。同时，英特尔® TDX 技术使用便捷，客户能在阿里云环境中大规模部署并实现实时迁移，拥有更灵活和友好的保密云计算环境。

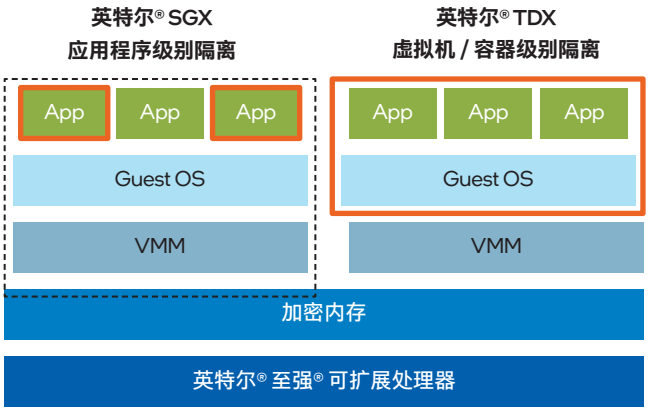
背景概述

不同类型的云计算服务，包括 IaaS、PaaS、软件即服务 (Software as a Service, SaaS) 以及功能即服务 (Functions as a Service, FaaS) 等，正在更多行业和领域中担当重任。这一过程中，包括阿里云在内的众多云服务提供商都将“在云环境中更有效地保护客户的数据资产”作为关注的焦点，并展开了诸多行动。而伴随云服务逐渐成为各类企业核心业务系统的 IT 基座，系统在云环境中运行时的数据保护，同样受到了越来越多的关注。

众所周知，云环境中的数据按其所处状态，可分为三类，即 Data in Transit（传输状态）、Data at Rest（存储状态）以及 Data in Use（使用状态）。对于前两种状态，云服务提供商正借助安全访问、数据加密以及各类加密传输协议等技术来为客户打造更为安全可信的云端环境。而对于使用状态中的数据，机密计算是实现其有效保护的良策。

机密计算为客户敏感数据提供了基于硬件的 TEE 环境，通过隔离保护的方式来防止未经授权的入侵者访问或修改处理中的数据，从而成为了目前云服务中常见的、面向应用运行时的数据安全技术方案。

作为机密计算技术的重要引领者，英特尔在数年前就推出了英特尔® 软件防护扩展（英特尔® Software Guard Extensions，英特尔® SGX）技术， 通过构建可信的“飞地（Enclave）”来为云环境应用程序中的敏感数据提供增强的安全防护。



图一 英特尔® SGX 与英特尔® TDX

如图一所示，英特尔® SGX 技术提供的可信边界是应用程序级的，客户需要面向云环境中不同的应用程序分别构建各自的安全环境。而随着云服务模式的日益多样化，更多企业客户也希望根据自身业务系统的需求，以及云基础设施的不同特性来构建具有不同可信边界级别的 TEE 环境，例如虚拟机、容器或应用程序，用以确保整体的数据机密性和完整性。

针对上述需求，阿里云与合作伙伴英特尔一起，基于其强大的云计算技术积累，在全新的第八代企业级 ECS 实例 g8i 中引入了第四代英特尔® 至强® 可扩展处理器。新一代处理器所内置的英特尔® TDX 技术与 ECS g8i 实例搭载的可信平台模块（Trusted Platform Module，TPM）安全芯片相配合，可为大型互联网、新金融、医疗保健、知识产权等业务场景提供更高安全等级的数据保护能力和云上可信运行环境，进一步帮助客户实现数据可用不可见的愿景。

解决方案

作为阿里云面向游戏、视频直播、电商、金融、医疗等诸多行业推出的新一代企业级弹性计算实例，阿里云第八代企业级 ECS 实例 g8i 创新地采用了“云基础设施处理器（Cloud Infrastructure Processing Units，CIPU）+ 飞天”的技术架构，并引入第四代英特尔® 至强® 可扩展处理器作为核心算力引擎，不仅性能相比上一代实例提升 60% 以上[1]，在深度学习、人工智能（Artificial Intelligence, AI）推理训练、大数据等应用场景中也有显著的能力跃升，同时其还在全球范围率先支持基于英特尔® TDX 技术的机密虚拟机能力，在云服务安全性方面获得了新的突破。

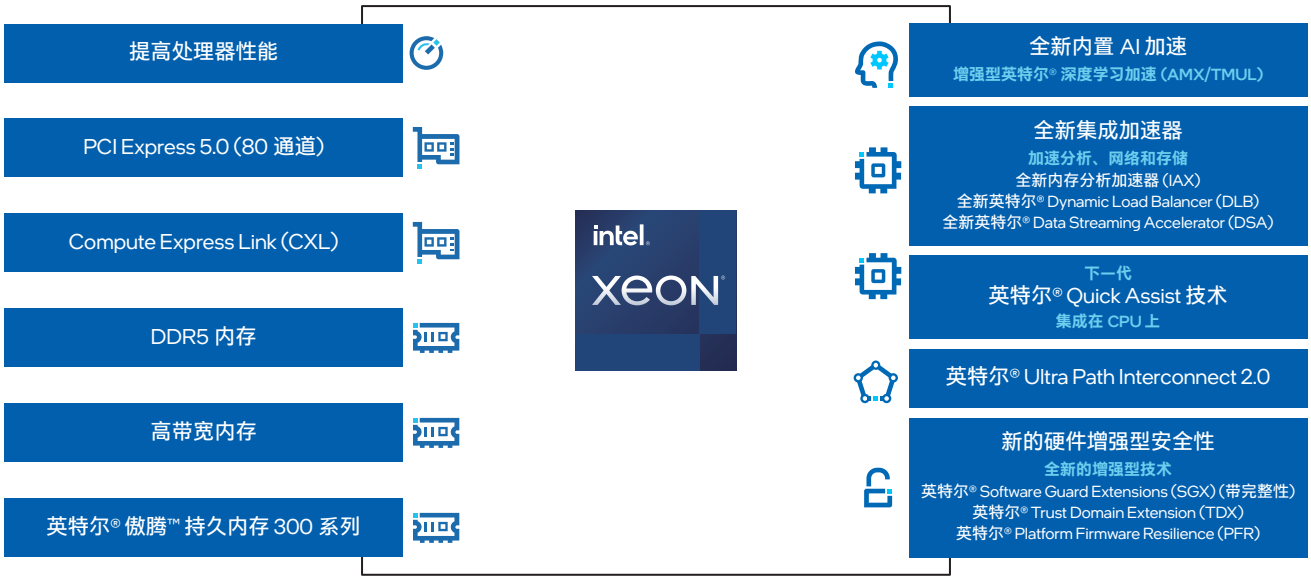
■ 通用及整体化性能双提升

得益于第四代英特尔® 至强® 可扩展处理器拥有的澎湃算力，以及英特尔® 高级矩阵扩展（Intel® Advanced Matrix Extensions，英特尔® AMX）、英特尔® 存内分析加速器（Intel® In-Memory Analytics Accelerator，英特尔® IAA）等提供的性能加持，新实例在各类云服务应用场景中都有着出色的性能表现，例如在深度学习训练场景中，性能较上一代实例提升 2 倍以上，推理性能则提升 4 倍；而在 RocksDB 等数据存储工作负载中，性能较上一代提升 1 倍以上[2]。

■ 全方位计算安全防护体系

面向企业核心业务上云的安全需求，新实例也提供了全面的防护加强。作为亚太地区最早部署机密计算的云服务提供商，阿里云一直以来都在开展机密计算技术推广。在其上一代 ECS 云实例（包括 g7t、c7t 和 r7t 安全增强型实例）中，就已经通过引入英特尔® SGX，以“飞地”的形式在内存中为客户应用程序开辟出可信的 TEE 环境，更好地保证了重要代码和数据的机密性与完整性。

随着更多企业级业务系统与云服务相融合，阿里云也看到客户的大多数应用程序或工作负载都是以虚拟机或容器的方式



图二 第四代英特尔® 至强® 可扩展处理器

部署到云环境中，并需要获得更大的可信边界。例如在金融、医疗等数据敏感性行业，客户往往希望其整个云环境，包括虚拟机、容器和应用程序中的数据都能处于机密计算环境的保护下。

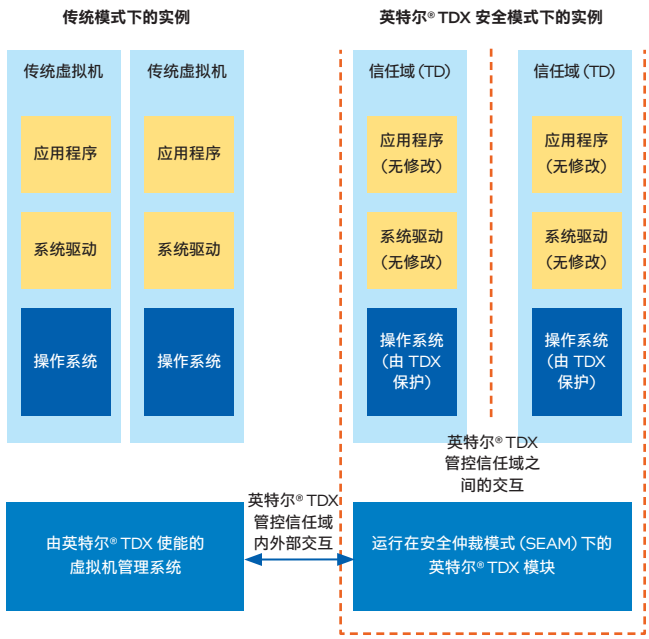
因此单一使用英特尔® SGX 提供的应用程序级可信边界，不仅会增加客户将全部应用程序、工作负载部署到安全云环境的难度，同时逐一对应用程序、工作负载开展改造，也会带来巨大的工作量。此时，阿里云等云服务提供商就需要寻求一种具有弹性可信边界、且易于将应用程序部署在其中的分级机密计算新方案。

而由第四代英特尔® 至强® 可扩展处理器内置的英特尔® TDX 技术，与阿里云新实例搭载的 TPM 安全芯片相配合，并结合阿里云自研的加密计算隔离环境 enclave，为阿里云第八代企业级 ECS 实例 g8i 构建了一个基于虚拟化的硬件可信环境，即为整个虚拟化实例 (包括虚拟机、容器) 都构建出可信的边界，由此为客户提供了可信边界更大、更易部署的安全云环境。

- **基于英特尔® TDX，构建全新的 TEE 环境和机密计算方案**

构建硬件 TEE 环境的关键，是对内存中的敏感数据提供可靠的隔离和保护措施。由第四代英特尔® 至强® 可扩展处理器内置内存控制器提供的内存加密引擎，可以让客户在不修改系统和应用程序软件的情况下，使用临时密钥对运行中的内存数据进行加密，从而使敏感数据始终处于加密隔离状态。

如图三所示，借助英特尔® 虚拟机扩展 (Intel® Virtual Machine Extension，英特尔® VMX) 技术与英特尔® 多密钥全内存加密 (Intel® Multi-Key Total Memory Encryption，英特尔® MK-TME) 技术，英特尔® TDX 为云实例提供了一种被称为“信任域 (Trust Domain，TD)”的全新虚拟访客环境。TD 可与其它 TD、实例，以及底层系统软件、管理软件实现相互隔离。而这些安全策略的实施，是由运行在安全仲裁模式 (Secure-Arbitration Mode，SEAM) 下的 TDX 安全服务模块来完成。



图三 英特尔 ® TDX 技术架构

这一架构中，英特尔® TDX 借助英特尔® MK-TME 技术为 TD 提供了数据机密性和完整性。英特尔® MK-TME 技术支持使用多种密钥对内存进行加密：

- 一方面，其提供的私密密钥，可用于对专用内存（放置 TD 的机密数据）进行加密；
- 另一方面，其提供的共享密钥则用于对共享内存进行加密，用于与 TD 外部的代理进行通信，以执行 I/O 操作，如网络访问、存储服务、调用管理程序服务等。

作为一种全新的机密计算技术，英特尔® TDX 使 TEE 环境的可信边界获得了有效扩展，从而让不同类型下的云服务，无论是 IaaS 或是 PaaS 中的云工作负载都能通过英特尔® TDX 整体纳入机密计算的数据保护之下。一般地，客户可以选择运行两种常用的机密计算方案，机密虚拟机（TD VM）和机密容器（TD CC）。机密虚拟机是运行在 TD 中的虚拟机实例，而机密容器是将机密计算与云原生容器集成，以保护 Kubernetes 上运行的敏感数据和应用程序。

阿里云第八代企业级 ECS 实例 g8i 可为客户提供机密虚拟机和机密容器两种使用模式：

1. **机密虚拟机：**作为全球首个基于英特尔® TDX 的公共云实例服务，客户可以按需订购机密计算环境，并通过英特尔® TDX 提供的“Lift-and-Shift（直接迁移）”方法，将传统应用程序升级为机密计算应用程序。此外，客户还可以通过利用远程认证功能（如实例内的磁盘加密等）来构建更加安全的解决方案。此外，双方还合作将英特尔® TDX 引入了阿里云创建的开源 Linux 发行版 OpenAnolis 中；
2. **机密容器：**由阿里云新实例提供的机密容器构建的基于虚拟化实例的 TEE 环境，能将特定容器组（例如 POD）与其他容器组及底层管理程序实现隔离以更好地保证数据安全性。同时双方也正推动基于 CoCo（云原生计算基金会“ CNCF ”的一个机密容器沙盒项目）的解决方案成为 OpenAnolis 的一部分。

无论哪种方式，客户都可以在云实例中轻松地搭建起自己的应用程序和数据，并受到可信赖的安全保护，使应用程序与数据都与外部环境隔离，以防止未经授权的访问。

英特尔® TDX 更多优势

为了让客户更便捷地实现云工作负载在安全环境中的部署，并更有效地保护敏感数据的使用、存储和传递，英特尔® TDX 还为客户提供了以下优势特性：

- 提供一系列“Lift-and-Shift（直接迁移）”的方法，用于将负载从传统模式的实例迁移到英特尔® TDX 安全模式的实例中而无需更改代码；
- 支持 TD 的整体迁移，即在业务不中断的前提下，将运行中的 TD 从源 TDX 平台实时迁移到目标 TDX 平台，这可以帮助阿里云实现更好的客户服务水平协议（Service Level Agreement，SLA），并满足其云服务在可升级性、可维护性等方面的要求；
- 提供对远程认证功能的支持，这一功能可用于证实 TD 在 TEE 环境中的运行过程，以及 TD 中运行的内容是可信的。

应用与展望

随着云服务安全关注度的不断提升，阿里云与英特尔都深刻地意识到，促进机密计算的技术发展和普及，应用和生态也是非常关键的一环。因此，双方已在多个领域携手开展基于英特尔® TDX 技术的云服务安全实践。

例如在 AI 领域，许多企业客户计划借助分布在云平台中充沛且来源丰富的数据，通过对多源数据开展机器学习建模与训练，在不同场景中打造更具时效性和可用性的 AI 应用。但出于数据隐私保护考虑，这些方案的制订一直受到掣肘。而英特尔® BigDL 隐私保护机器学习（Intel® BigDL Privacy-Preserving Machine Learning，英特尔® BigDL PPML）可以在英特尔® TDX 技术的加持下实现对分布式节点或 AI 管道的保护，从而让客户在不牺牲数据隐私的前提下将更多的数据运用到 AI 应用中，有效挖掘数据价值。目前，阿里云与英特尔已通过融合英特尔® TDX 技术、机密虚拟机以及机密容器，为客户构建更为高效的隐私保护机器学习方案。

（如欲了解更多应用细节，请访问：https://developer.aliyun.com/article/1081960）

为客户提供有效的数据安全和隐私保护，是阿里云等云服务提供商最重要的原则之一，而由第四代英特尔® 至强 ® 可扩展处理器、英特尔® TDX 技术以及一系列阿里云安全服务提供的数据保护矩阵，正帮助客户通过定制化的机密计算解决方案，实现更加可靠的云端数据资产保护。面向未来，阿里云还将与英特尔进一步展开深入合作，为更多行业和领域的客户构建更加安全、开放和高可靠性的云计算基础设施。

[1]数据援引自公开媒体报道：https://developer.aliyun.com/article/1114031

[2]数据来源于阿里云，如欲了解更多详情，请联系阿里云：https://www.aliyun.com/