SaaS 多租户数据如何隔离

SaaS 基于多租户架构，一个 SaaS 中会有多个用户的数据保存在同一个数据存储位置。SaaS 供应商应保证任何一个用户在访问数据时不能访问到其他用户的数据，因此供应商需要在 SaaS 的应用体系和数据模型的设计上确保数据隔离。

微软 Azure 为每个部署提供了网络隔离功能，通过使用 input endpoint，可以控制哪些端口能够从互联网访问。

（1）虚拟机之间的通讯始终通过可信赖的数据包筛选器进行。

a. 地址解析协议（ARP）和动态主机配置协议（DHCP）等协议，以及来自虚拟机的其他 OSI 第二层通讯都可使用速率限制和反欺骗保护进行控制。

b. 虚拟机无法捕获任何目标地址非自己的网络通讯。

（2）客户的虚拟机无法将通讯发往 Azure 的私有接口或其他客户的虚拟机，也无法发往 Azure 基础架构服务。客户的虚拟机只能与相同客户所拥有或控制的虚拟机、以及用于公共通讯的 Azure 基础架构服务终结点通讯。

（3）当客户将虚拟机放入虚拟私有网络后，这些虚拟机将获得自己的、完全不可见的地址空间，此时将无法从部署或虚拟网络之外的虚拟机访问（除非通过公共 IP 地址配置为可见）。

如果想了解更多，欢迎来电咨询

电话：010-82676188

邮箱：market@neotrident.com

官网：www.neotrident.com