Microsoft Azure China 上手手册

Contents

1. 前言

在微软实际工作中，客户经常会问是否有个快速了解 Azure 的手册，Azure Global 和 Azure China 都有内容全面的官网，出于从认知的角度去帮助用户快速认识并使用 Azure，本文集结了架构师编写了 Azure China 基础服务的上手手册。本手册以 Azure 架构师张磊 2015 年的版本为基础进行改版，把笔者（刘劲男、司徒志恒、黄旭、黄龙飞）认为重要的常用基础功能给大家做个初步介绍，以 Azure China 为主。

本文分成概念篇、操作篇、运维篇，读者可以各取所需，也可以从头开始了解并按文档进行上手操作。由于笔者时间、认知有限，如有纰漏欢迎大家指正。且随着 Azure 新功能的不断发布，此手册内容仅为导入式学习材料，Azure 实际功能和更新内容以官网为准。

2. 什么是 Azure?

Azure 云平台包含 200 多个产品和云服务，旨在帮助您将新的解决方案引入生活，解决当今的挑战并创造未来。使用您选择的工具和框架，跨多个云、本地和边缘构建、运行和管理应用程序。

Microsoft Azure 是微软的公有云平台，在中国大陆，Microsoft Azure 由世纪互联独立运营，与全球其他地区由微软运营的 Azure 服务在物理上和逻辑上独立，采用微软服务于全球的 Azure 技术，为客户提供全球一致的服务质量保障。所有客户数据、处理这些数据的应用程序，以及承载世纪互联在线服务的数据中心，全部位于中国境内。位于中国东部 和中国北部的数据中心在距离相隔 1000 公里以上的地理位置提供异地复制，为 Azure 服务提供了业务连续性支持，实现了数据的可靠性。

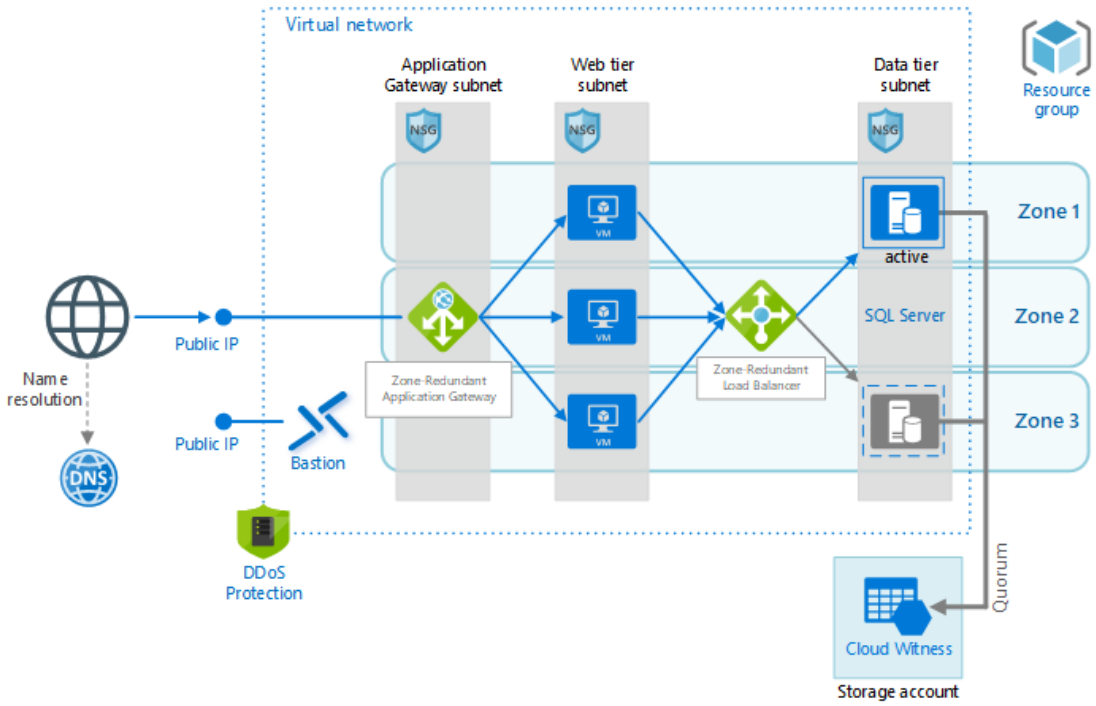
在网络接入方面，世纪互联运营的 Microsoft Azure 的数据中心通过 BGP 方式直接连接多家主流运营商（中国电信、中国联通、中国移动）的省级核心网络节点，可为用户提供高速稳定的网络访问体验。位于中国东部和北部的数据中心采用相同的地址广播和 BGP 路由策略，用户可以就近访问位于上述数据中心的 Azure 服务，达到最佳网络性能体验。

所有数据中心选取国内电信运营商的顶级数据中心，在绿色节能的基础上，采用 N+1 或者 2N 路不间断电源保护。此外还有大功率柴油发电机为数据中心提供后备电力，配有现场柴油存储和就近加油站的供油协议作为保障。数据中心机房内均设有架空地板，冷通道封闭，与后端制冷系统，冷机，冷却塔和冰池形成高效冷却循环，为机房内运行的服务器提供稳定适合的环境。并配有新风系统，可在天气条件适合时最大限度地降低数据中心的 PUE 。

在安全性方面，我们保证客户数据的安全。Azure 采用一系列可靠的安全技术和实践，帮助确保 Azure 基础结构能够**应对攻击**，保护用户对 Azure 环境的访问，并通过加密通信、威胁管理和缓解实践（包括定期渗透测试）来帮助保障客户数据的安全。业界一流的安全技术和流程确保客户数据的机密性、完整性和可用性，提供有财务保障的最高达 99.99% 的月度服务级别协议，可提供最多 6 个数据备份。

客户拥有并控制自己的客户数据。客户全权管理自己的客户数据以及权限，决定客户数据的存储位置。未经批准任何人都无法使用客户数据。不同租户的客户数据在逻辑上进行了彻底的隔离，客户数据不会被用于广告宣传或者其他商业目的。我们符合全球以及国内的标准。满足国际和行业特定标准 ISO/IEC27001，公安部信息系统安全等级保护评定第三级备案，以及多项可信云服务认证。严格的第三方审计验证了 Azure 可以满足不同标准强制要求的安全控制。作为我们对透明度的承诺，您可以通过向进行认证的第三方索要审计结果，来验证我们对众多安全控制的实现情况。客户可以清楚了解数据是如何被存储和访问的，并知道我们如何保护它们的。首家推出公开服务仪表盘，提供透明可信的服务保障。通过可访问的工具和简洁直观的语言， 以透明的方式披露客户数据的存储位置、可以访问的人员，以及世纪互联用何种方法保护客户数据，由世纪互联运营的 Microsoft Azure 可以帮助客户更好地控制自己的客户数据。客户清楚知道自己的客户数据的存储位置，客户数据是如何被使用、管理和保护的。

本文档以搭建一个简单应用为背景,对 Azure 计算、存储、网络等关键基础架构服务展开详细介绍,适合刚接触 Azure 的技术相关角色作为上手指南参考。



注：示例架构图中可用性区域(Zone)在 Azure China 目前尚未提供，可以使用可用性集实现 VM 的高可用性，具体可参考下文 3.1.6 虚拟机的高可用性部分

3. Azure 基础服务介绍

3.1 Azure 虚拟机相关介绍

3.1.1 操作系统

Azure 虚拟机在创建的过程中，都需要用户选择操作系统的版本。创建完的虚拟机默认都安装好了操作系统。

微软 Azure 官方支持的操作系统为：

1. Windows : Server 2008 R2, Server 2012, Server 2012 R2, Windows Server 2016, Windows Server 2016 Core

2. SQL Server：SQL Server 2008 R2, SQL Server 2012 SP1, SQL Server 2014 RTM (Web, Standard, Enterprise), SQL Server 2016

3. Linux：Azure 认可的 Linux 分发 | Azure Docs

4. 其他非 Azure 提供的虚拟机模板，比如 RedHat 或者红旗 Linux。客户可以自己在本地使用 Hyper-V 进行创建，然后上传至 Azure 云端。

3.1.2 虚拟机规格

Azure 提供了丰富的虚拟机规格族以及不同资源配比的型号供选择,具体型号可参考以下链接；

Windows 操作系统

- 常规用途：https://docs.azure.cn/zh-cn/virtual-machines/sizes-general?toc=/virtual-machines/windows/toc.json&bc=/virtual-machines/windows/breadcrumb/toc.json
- 计算优化：https://docs.azure.cn/zh-cn/virtual-machines/sizes-compute?toc=/virtual-machines/windows/toc.json&bc=/virtual-machines/windows/breadcrumb/toc.json
- 内存优化：https://docs.azure.cn/zh-cn/virtual-machines/sizes-memory?toc=/virtual-machines/windows/toc.json&bc=/virtual-machines/windows/breadcrumb/toc.json
- GPU 加速：https://docs.azure.cn/zh-cn/virtual-machines/sizes-gpu?bc=/virtual-machines/windows/breadcrumb/toc.json&toc=/virtual-machines/windows/toc.json

Linux 操作系统

- 常规用途：https://docs.azure.cn/zh-cn/virtual-machines/sizes-general?toc=/virtual-machines/linux/toc.json&bc=/virtual-machines/linux/breadcrumb/toc.json
- 计算优化：https://docs.azure.cn/zh-cn/virtual-machines/sizes-compute?toc=/virtual-machines/linux/toc.json&bc=/virtual-machines/linux/breadcrumb/toc.json
- 内存优化：https://docs.azure.cn/zh-cn/virtual-machines/sizes-memory?toc=/virtual-machines/linux/toc.json&bc=/virtual-machines/linux/breadcrumb/toc.json
- GPU 加速：https://docs.azure.cn/zh-cn/virtual-machines/sizes-gpu?toc=/virtual-machines/linux/toc.json&bc=/virtual-machines/linux/breadcrumb/toc.json

3.1.3 虚拟机磁盘

在 Azure 中有三个主要磁盘角色：数据磁盘、OS 磁盘和临时磁盘。 这些角色将映射到附加到虚拟机的磁盘。

OS 磁盘

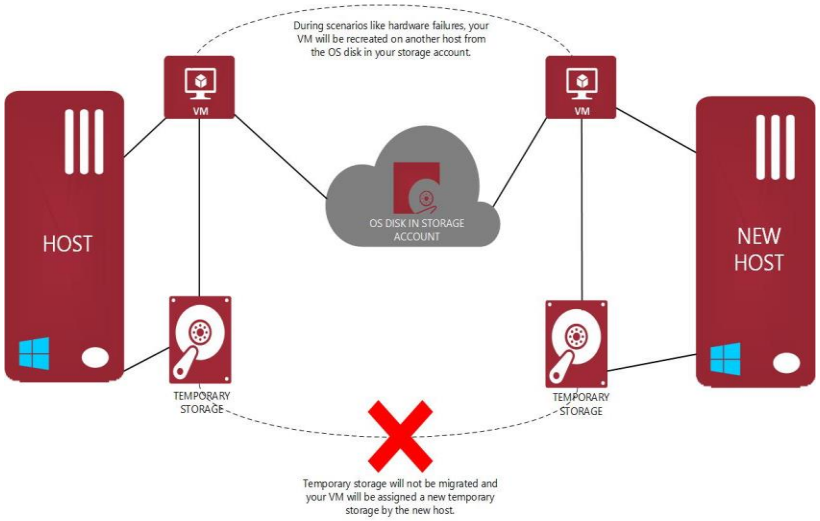
每个虚拟机都附加了一个操作系统磁盘。 该 OS 磁盘有一个预先安装的 OS，是在创建 VM 时选择的。 此磁盘包含启动卷。此磁盘最大容量为 4,095 GiB。

临时磁盘

大多数 VM 都包含一个临时磁盘，该磁盘不是托管磁盘。 临时磁盘为应用程序和进程提供短期存储，仅用于存储页面或交换文件等数据。

数据磁盘

数据磁盘是附加到虚拟机的托管磁盘，用于存储应用程序数据或其他需要保留的数据。 数据磁盘注册为 SCSI 驱动器并且带有所选择的字母标记。 每个数据磁盘的最大容量为 32,767 gibibytes (GiB)。 虚拟机的大小决定了可附加的磁盘数目，以及可用来托管磁盘的存储类型。



注意事项

不要使用临时磁盘来存储数据，Windows 操作系统的虚拟机临时磁盘默认是 D：驱动器，linux 操作系统的虚拟机临时磁盘默认是/dev/sdb1。 它只是临时存储空间，因此存在丢失数据且数据不能恢复的风险。 将虚拟机移到另一主机时，可能会发生数据丢失的情况。 调整虚拟机大小、更新主机、主机硬件故障等都是需要移动虚拟机的原因。

对于数据存储，我们建议存放在挂载在虚拟机上的托管磁盘。关于托管的介绍，请参考本文 3.2.1.2 托管磁盘介绍。

3.1.4 虚拟机存储空间

每个数据磁盘的容量高达 32,767 GiB。 可以使用的数据磁盘数取决于虚拟机大小。 有关详细信息，请参阅 3.1.2 虚拟机规格中的虚拟机规格参数文档链接。

Azure 托管磁盘是推荐用于 Azure 虚拟机的磁盘存储产品，方便永久存储数据。 可对每个虚拟机使用多个托管磁盘。 托管磁盘提供两种类型的持久存储选项：高级和标准托管磁盘。

托管磁盘具有以下优势:

- 高度持久和可用：提供三个包含数据的副本，确保高持久性。 如果其中一个或两个副本出现问题，剩下的副本能够确保数据的持久性和对故障的高可用性。
- 简单且支持 VM 弹性部署
- 集成可用性集：托管磁盘集成可用性集，可确保可用性集中的 VM 的磁盘彼此之间完全隔离以避免单点故障。
- 支持通过 Azure backup 备份还原
- 支持服务器端加密 (SSE)或 Azure 磁盘加密 (ADE)：服务器端加密可提供静态加密并保护数据，让你的组织能够信守安全性与合规性方面所做的承诺。 默认情况下，所有托管磁盘、快照和映像都启用了服务器端加密，但不会加密临时磁盘；Azure 磁盘加密允许加密 IaaS 虚拟机使用的 OS 磁盘和数据磁盘， 此加密包括托管磁盘。

如何选择合适的 VM 托管磁盘类型，可参考：选择 Azure IaaS Linux VM 的磁盘类型 - 托管磁盘 | Azure Docs

3.1.5 远程连接虚拟机

使用适用于 Windows VM 的远程桌面连接 (RDP) 建立远程连接。 有关说明，请参阅如何连接并登录到运行 Windows 的 Azure 虚拟机。 除非将服务器配置为远程桌面服务会话主机，否则最多支持两个并发连接。

使用安全外壳 (SSH) 建立访问 Linux VM 的远程连接，以登录到虚拟机。 请参阅如何从 Windows 或从 Linux 和 Mac 进行连接的相关说明。 默认情况下，SSH 允许的并发连接最多为 10 个。 通过编辑配置文件，可以增加此数量。

另外，需要注意首先需要确保被访问的 VM 关联了一个 Internet 可达的公网 IP 地址，并且拥有适当的安全组设置，远程访问请求和会话没有被阻止。关于虚拟网络的公网 IP 地址请参考本文 3.3.2 子网和 IP 地址部分。关于安全组请参考本文 3.3.3 网络安全组部分。

3.1.6 虚拟机的高可用性

Azure 为承载于虚拟机上且需要高可用和弹性的业务提供了高可用和弹性的架构和功能，工作负荷通常分布在不同的虚拟机上，以获得高吞吐量、高性能并实现冗余，防止 VM 因更新或其他事件而受影响。

3.1.6.1 容错域

容错域是共享公用电源和网络交换机的基础硬件逻辑组，类似于本地数据中心内的机架。

3.1.6.2 更新域

更新域是可以同时维护或重新启动的基础硬件逻辑组。

Azure 平台进行定期维护时，此方法可确保至少有一个应用程序实例始终保持运行状态。 在维护期间，更新域的重启顺序可能不会按序进行，但一次只重启一个更新域。

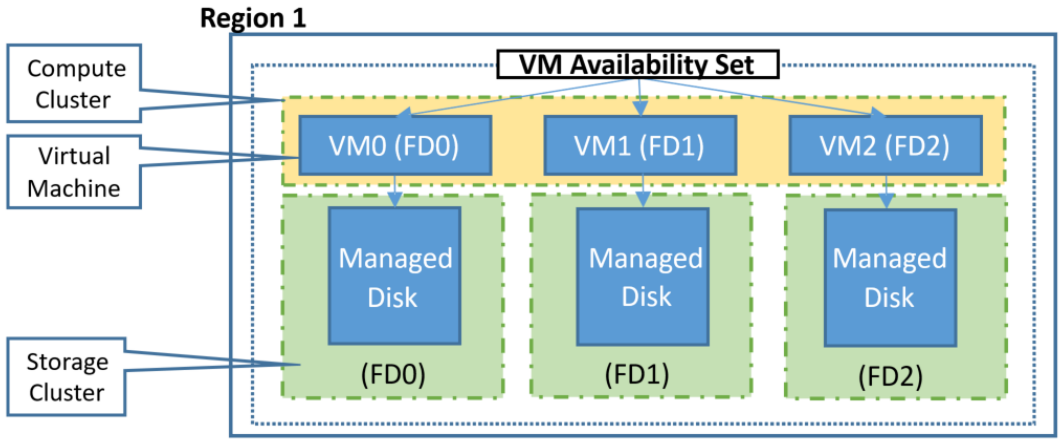
3.1.6.3 可用性集

可用性集是数据中心内的 VM 的逻辑分组，可让 Azure 了解应用程序的构建方式，以便提供冗余和可用性。 建议在可用性集内创建两个或多个 VM，提供高度可用的应用程序，并满足 99.95% Azure SLA 的要求。 可用性集本身是免费的，只需为创建的每个 VM 实例付费。 当单个 VM 使用 Azure 高级 SSD 时，Azure SLA 适用于计划外维护事件。

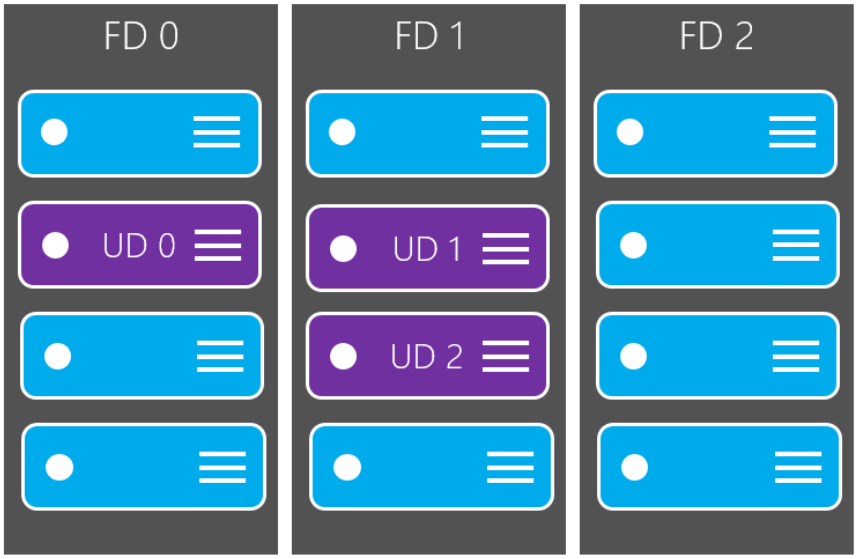
在可用性集中，VM 自动分布到这些容错域中。 此方法可限制潜在物理硬件故障、网络中断或断电的影响。

对于使用 Azure 托管磁盘的 VM，在使用托管可用性集时，VM 与托管磁盘容错域一致。 该一致性可确保附加到 VM 的所有托管磁盘都在同一托管磁盘容错域内。

在托管可用性集中，只能创建带托管磁盘的 VM。 托管磁盘容错域的数目因区域而异 - 每个区域两个或三个托管磁盘容错域。 可以阅读有关这些适用于 Linux VM 或 Windows VM 的托管磁盘容错域的详细信息。



可用性集中的 VM 也会自动分布到更新域中：下图中 FD 指容错域，UD 指更新域。



3.1.6.1 虚拟机规模集

使用 Azure 虚拟机规模集可以创建并管理一组负载均衡的 VM。 可以根据需求或定义的计划自动增减 VM 实例的数目。 规模集为应用程序提供高可用性，用于集中管理、配置和更新许多 VM。 建议在一个规模集内创建两个或多个 VM，使应用程序高度可用，并满足 99.95% Azure SLA 的要求。 规模集本身是免费的，你只需为创建的每个 VM 实例付费。 当单个 VM 使用 Azure 高级 SSD 时，Azure SLA 适用于计划外维护事件。 规模集内的虚拟机可以跨多个更新域和容错域部署，以最大程度地提高因数据中心中断、计划内或计划外维护事件而导致停机时的可用性和复原能力。

3.1.7 虚拟机 SLA

如上一节描述，Azure 提供了多种满足高可用的弹性架构，对于单机部署和高可用架构部署的虚拟机，Azure 同样提供了对应的 SLA 承诺：

- 对于在同一 Azure 区域中跨两个或更多可用性区域部署了两个或多个实例的所有虚拟机，我们保证您可在不少于 99.99% 的时间内与至少一个实例具有虚拟机连接性。（仅适合 Azure Global）
- 对于在同一可用性集或同一专用主机组中部署了两个或两个以上实例的所有虚拟机，我们保证您在不少于 99.95% 的时间内与至少一个实例具有虚拟机连接性。(Azure China 目前仅提供可用性集)
- 对于所有操作系统磁盘和数据磁盘均使用高级 SSD 或超级磁盘的任一单实例虚拟机，我们均保证您将在不少于 99.9% 的时间内具有虚拟机连接性。(Azure China 目前仅提供高级 SSD)
-
- 对于操作系统磁盘和数据磁盘均使用标准 SSD 托管磁盘的任一单实例虚拟机，我们保证您将在不少于 99.5% 的时间内具有虚拟机连接性。
- 对于操作系统磁盘和数据磁盘均使用标准 HDD 托管磁盘的任一单实例虚拟机，我们保证您将在不少于 95% 的时间内具有虚拟机连接性。

详细 SLA 介绍和条款细则可参考：[虚拟机的服务级别协议 | Azure]

3.2 Azure 存储服务介绍

Azure 存储平台是 Microsoft 提供的适用于现代数据存储方案的云存储解决方案。 核心存储服务为数据对象提供可大规模缩放的对象存储、为 Azure 虚拟机 (VM) 提供磁盘存储、为云提供文件系统服务，并且提供用于可靠消息传送的消息传送存储以及 NoSQL 存储。 这些服务包括：

- 持久且具有高可用性。 冗余可确保数据在发生短暂的硬件故障时是安全的。 还可以选择在各个数据中心或地理区域之间复制数据，从而在发生本地灾难或自然灾害时提供额外的保护。以此方式复制的数据在发生意外中断时将保持高可用性。
- 安全。 该服务会对写入到 Azure 存储帐户的所有数据进行加密。 Azure 存储可以精细地控制谁可以访问你的数据。
- 可缩放。 Azure 存储设计为可大规模缩放以满足当今的应用程序在数据存储和性能方面的需求。
- 托管的。 Azure 为你处理硬件维护、更新和关键问题。
- 易访问。 可以通过 HTTP 或 HTTPS 从世界上的任何位置访问 Azure 存储中的数据。Microsoft 以各种语言（包括 NET、Java、Node.js、Python、PHP、Ruby、Go 和其他语言）提供了适用于 Azure 存储的客户端库以及成熟的 REST API。 Azure 存储支持通过 Azure PowerShell 或 Azure CLI 运行脚本。 而且，Azure 门户和 Azure 存储资源管理器提供了用于处理数据的简单可视化解决方案。

3.2.1 存储服务分类

Azure 包含以下几种核心存储服务，每个服务的访问都通过存储帐户进行:

- Azure Blob：适用于文本和二进制数据的可大规模缩放的对象存储。 还包括通过 Data Lake Storage Gen2 支持大数据分析。
- Azure 文件：适用于云或本地部署的托管文件共享。
- Azure 队列：用于在应用程序组件之间进行可靠的消息传送的消息存储。
- Azure 表：一种 NoSQL 存储，适合用作结构化数据的无架构存储。
- Azure 托管磁盘：Azure VM 的块级存储卷。

3.2.1.1 Blob 存储

Azure Blob 存储是 Microsoft 提供的适用于云的对象存储解决方案。 Blob 存储最适合存储巨量的非结构化数据，例如文本或二进制数据。

Blob 存储最适合用于:

- 直接向浏览器提供图像或文档。
- 存储文件以供分布式访问。
- 对视频和音频进行流式处理。
- 存储用于备份和还原、灾难恢复及存档的数据。
- 存储数据以供本地或 Azure 托管服务执行分析。

详细介绍可参考: https://docs.azure.cn/zh-cn/storage/blobs/storage-blobs-introduction/

3.2.1.2 托管磁盘

Azure 托管磁盘是虚拟硬盘 (VHD)。 可以将其视为本地服务器中的物理磁盘，但它是虚拟化的。 Azure 托管磁盘作为页 blob 存储，后者是 Azure 中的随机 IO 存储对象。 我们之所以将托管磁盘称为“托管”是因为，它与传统非托管磁盘相比，提供了存储可用性集和存储账户的手工配置的限制，所以大大提高了磁盘高可用性。 对于托管磁盘，你所要做的就是预配磁盘，而 Azure 负责其余的工作。

有关托管磁盘的详细信息，请参阅 Azure 托管磁盘简介。

3.2.1.3 表存储

Azure 表存储现在是 Azure Cosmos DB 的一部分。 若要查看 Azure 表存储文档，请参阅 Azure 表存储概述。 除了现有的 Azure 表存储服务，还有新的 Azure Cosmos DB 表 API 产品/服务，后者提供吞吐量优化表、全局分发和自动辅助索引。 要详细了解并尝试新的高级体验，请查看 Azure Cosmos DB 表 API (aka.ms)。

有关表存储的详细信息，请参阅 Azure 表存储概述。

3.2.1.4 队列存储

Azure 队列服务用于存储和检索消息。 队列消息最大可以为 64 KB，一个队列可以包含数百万条消息。 队列通常用于存储需要异步处理的消息的列表。

例如，假设你需要客户能够上传图片，并且你需要创建每个图片的缩略图。 可以让客户在上传图片时等待你创建缩略图， 也可以使用队列。 当客户完成上传操作后，向队列写入一条消息。 然后通过 Azure Function 从队列检索该消息并创建缩略图。 此处理过程的每一部分都可以单独进行缩放，让你可以根据使用情况进行调整，加强控制。

有关 Azure 队列的详细信息，请参阅队列简介。

3.2.1.5 文件存储

可以通过 Azure 文件设置可用性高的网络文件共享，以便使用标准的服务器消息块 (SMB) 协议对其进行访问。 这意味着，多个 VM 可以共享启用了读取和写入访问权限的相同文件。 也可使用 REST 接口或存储客户端库来读取文件。

Azure 文件不同于公司文件共享的一点是，可以在全球任何地方使用 URL 来访问文件，只要该 URL 指向文件且包含共享访问签名 (SAS) 令牌即可。 可以生成 SAS 令牌，用于在指定时间内对私有资产进行特定访问。

文件共享适用于许多常用方案：

- 许多本地应用程序使用文件共享。 此功能可以更方便地迁移那些将数据共享到 Azure 的应用程序。 如果将文件共享装载到本地应用程序所使用的驱动器号，则应用程序中访问文件共享的那部分应尽量少做更改（如果必须进行更改的话）。
- 配置文件可以在一个文件共享上存储，从多个 VM 进行访问。 可以将一个组中多个开发人员使用的工具和实用程序存储到文件共享中，确保每个人都能找到它们并使用同一版本。
例如，资源日志、指标和故障转储是三种可以写入到文件共享供以后处理或分析的数据。

有关 Azure 文件的详细信息，请参阅 Azure 文件简介。

某些 SMB 功能不适用于云。 有关详细信息，请参阅 Features not supported by the Azure File service（Azure 文件服务不支持的功能）。

3.2.1.6 基于 blob 存储的数据湖

Data Lake Storage Gen2 使 Azure 存储成为在 Azure 上构建企业 Data Lake 的基础。 Data Lake Storage Gen2 从一开始就设计为存储数千万亿字节的信息，同时保持数百千兆位的吞吐量，允许你轻松管理大量数据。

Data Lake Storage Gen2 的一个基本部分是向 Blob 存储添加分层命名空间。 分层命名空间将对象/文件组织到目录层次结构中，以便进行有效的数据访问。 常见的对象存储命名约定在名称中使用斜杠来模拟分层目录结构。 这种结构在 Data Lake Storage Gen2 中得以真正实现。 诸如重命名或删除目录之类的操作在目录上成为单个原子元数据操作，而不是枚举或处理共享目录名称前缀的所有对象。

Data Lake Storage Gen2 在 Blob 存储的基础上构建，并通过以下方式增强了性能、管理和安全性：

- 优化了性能，因为你不需要将复制或转换数据作为分析的先决条件。 与 Blob 存储上的平面命名空间相比，分层命名空间极大地提高了目录管理操作的性能，从而提高了整体作业性能。
- 管理更为容易，因为你可以通过目录和子目录来组织和操作文件。
- 安全性是可以强制实施的，因为可以在目录或单个文件上定义 POSIX 权限。
- 另外，Data Lake Storage Gen2 非常经济高效，因为它构建在低成本的 Azure Blob 存储之上。这些新增功能进一步降低了在 Azure 上运行大数据分析的总拥有成本。

更多关于 Data Lake Storage Gen2 的信息，请参考 Azure Data Lake Storage Gen2 简介 | Azure Docs

3.2.2 存储账户类型

Azure 存储提供多种类型的存储帐户。 每种类型支持不同的功能，不同的性能和访问层，以及复制选项，并且具有自己的计费标准，不同存储服务所对应的计费标准可参考本文 4.4 存储成本分析部分。下图概述了存储账户类型及其提供的功能差异，用户可以根据实际需求选择合适的存储账户类型。

存储帐户类型	支持的服务	支持的性能层	支持的访问层	复制选项	部署模型 1	Encryption 2
常规用途 V2	Blob、文件、队列、表、磁盘和 Data Lake Gen2 5	标准、高级 5	热、冷、存档 3	LRS、GRS、RA-GRS	Resource Manager	加密
常规用途 V1	Blob、文件、队列、表和磁盘	标准、高级 4	空值	LRS、GRS、RA-GRS	资源管理器、经典	加密
BlockBlobStorage	Blob（仅块 Blob 和追加 Blob）	Premium	空值	LRS	Resource Manager	加密
FileStorage	仅文件	Premium	空值	LRS	Resource Manager	加密
BlobStorage	Blob（仅块 Blob 和追加 Blob）	标准	热、冷、存档 3	LRS、GRS、RA-GRS	Resource Manager	加密

3.2.3 存储冗余备份

本地冗余存储 (LRS) 在主要区域中的单个物理位置内同步复制数据三次。 LRS 是成本最低的复制选项，但对于需要高可用性的应用程序，不建议使用此选项。

异地冗余存储 (GRS) 使用 LRS 在主要区域中的单个物理位置内同步复制数据三次。 然后，它将数据异步复制到次要区域中的单个物理位置。如果主要区域不可用，可以选择故障转移到次要区域。 故障转移完成后，次要区域将成为主要区域，你便可以再次读取和写入数据。

异地冗余存储将数据复制到次要区域中的另一个物理位置，以防范区域性服务中断。 但是，仅当客户或 Azure 发起了从主要区域到次要区域的故障转移时，数据才可供读取。 启用对次要区域的读取访问时，如果主要区域不可用，则数据可供读取。 若要在主区域正常时对次要区域进行读取访问，请启用**读取访问异地冗余存储 (RA-GRS)**。

3.2.4 存储服务 SLA

参数	LRS	GRS/RA-GRS
给定一年内的对象持久性百分比[1]	至少 99.999999999%（11 个 9）	至少 99.99999999999999%（16 个 9）
读取请求的可用性 SLA[1]	至少为 99.9%（冷访问层为 99%）	GRS 至少为 99.9%（冷访问层为 99%） RA-GRS 至少为 99.99%（冷访问层为 99.9%）
写入请求的可用性 SLA[1]	至少为 99.9%（冷访问层为 99%）	至少为 99.9%（冷访问层为 99%）

详细 SLA 信息和条款可参考：[存储的服务级别协议 | Azure]

3.3 Azure 应用服务介绍

3.3.1 应用服务概述

Azure 应用服务是一项基于 HTTP 的服务，用于托管 Web 应用程序、REST API 和移动后端 。 可以使用 .NET、NET Core、Java、Ruby、Node.js、PHP 或 Python 等偏好的语言进行开发。 在基于 Windows 和 Linux 的环境中，应用程序都可以轻松地运行和缩放。

应用服务不仅可将 Microsoft Azure 的强大功能（例如安全性、负载均衡、自动缩放和自动管理）添加到应用程序。 还可以利用其 DevOps 功能，例如包管理、过渡环境、自定义域和 TLS/SSL 证书。

3.3.2 应用服务主要功能

多个语言和框架 - 应用服务针对 ASP.NET、ASP.NET Core、Java、Ruby、Node.js、PHP 或 Python 提供一流支持。 我们还能以后台服务的形式运行 PowerShell 和其他脚本或可执行文件。

托管生产环境 - 应用服务会自动 修补并维护 OS 和语言框架。 将时间花在编写优秀应用上，让 Azure 来考虑平台问题。

具有高可用性的全局缩放 - 以手动或自动方式进行 增大或 扩大。 在 Azure.cn 的全国数据中心基础结构中的任意位置托管应用，并且应用服务 SLA 承诺高可用性。

与 SaaS 平台和本地数据建立连接 - 从适用于企业系统（例如 SAP）的 50 多个 连接器、SaaS 服务（例如 Salesforce）以及 Internet 服务（例如 Facebook）中进行选择。 使用混合连接和 Azure 虚拟网络访问本地数据。

安全性和合规性 - 应用服务符合 ISO、SOC 和 PCI 的要求。 使用 Azure Active Directory 或 Microsoft 帐户对用户进行身份验证。 创建 IP 地址限制和管理服务标识。

应用程序模板 - 从 Azure 市场的大量应用程序模板列表中进行选择，例如 WordPress、Joomla 和 Drupal。

Visual Studio 与 Visual Studio Code 集成 - Visual Studio 和 Visual Studio Code 中的专用工具可简化创建、部署和调试工作。

API 和移动功能 - 应用服务针对 RESTful API 方案提供统包式 CORS 支持，通过启用身份验证、脱机数据同步、推送通知等功能简化移动应用方案。

无服务器代码 - 按需运行代码片段或脚本，无需显式预配或管理基础结构，并且只需为代码实际使用的计算时间付费（请参阅 Azure Functions）。

3.3.3 使用应用服务注意事项

创建应用服务时，将同时生成以 chinacloudsites.cn 结尾的默认域名，该域名仅可用于云平台内部各服务之间及各数据中心之间的通讯，任何通过互联网到应用服务之间的流量将会被自动封堵。如需通过互联网对应用服务进行访问，请您绑定一个已经完成 ICP 备案的自定义域名，通过该自定义域名进行访问。

自定义域名绑定方法

https://docs.azure.cn/zh-cn/app-service/app-service-web-tutorial-custom-domain

如果没有绑定自定义域名，

当您通过 Http 协议访问默认域名时，您将看到如下封堵页面。

温馨提示：该网站暂时无法进行访问

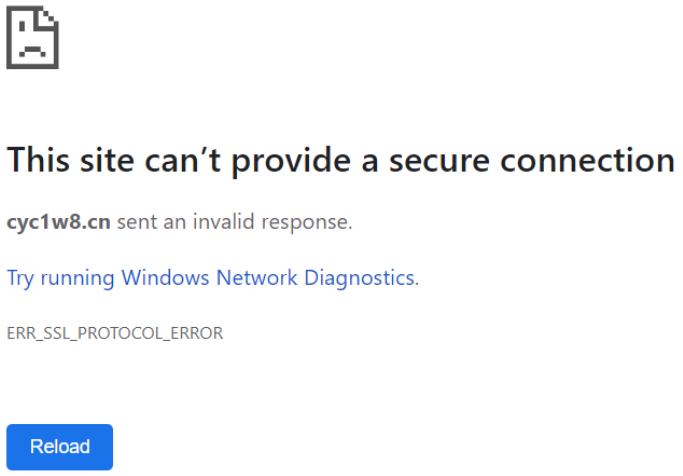
原因一：您尚未根据工信部相关法规申请经营许可或进行网站备案；
原因二：您未根据公安部相关法规完成公安备案；
原因三：网站内容与备案信息不符，建议网站管理员尽快修改网站信息；
原因四：您的网站可能存在不适宜传播的信息，请联系您的网站管理员。

本页面为默认提示页面，如网站存在以上问题请及时进行相关处理。
上海蓝云用户ICP备案请登录上海蓝云备案管理系统；
上海蓝云用户公安备案请登陆全国公安机关互联网安全管理服务平台；
谢谢合作！
Sorry, the website is unable to be accessed at this moment.
According to the ICP filling requirements of China's Ministry of Industry and Information Technology (MIIT) and China Public Security Ministry.
a website is accessible only if the registration is completed and the filled information is accurate.
In addition, the access should be suspended if any prohibited content is published or disseminated.

世纪互联
www.21vianet.com
上海蓝云网络科技有限公司

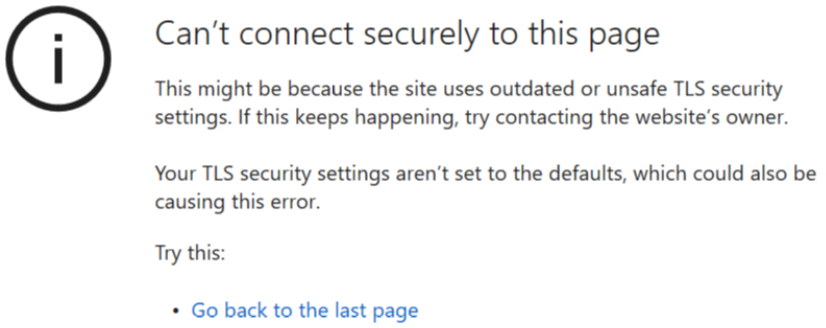
当您通过 Https 协议访问默认域名时，根据不同浏览器，您将看到如下不同报错：

Chrome 浏览器



Firefox 浏览器

IE Edge 浏览器



当您绑定一个已经完成 ICP 备案的自定义域名后，无需进行其他设置，即可通过该自定义域名访问应用服务。

3.4 Azure 网络基础服务介绍

3.4.1 虚拟网络(vnet)

Azure 虚拟网络 (VNet) 是对专用于订阅的 Azure 云进行的逻辑隔离，类似于在你在自己的数据中心运营的传统网络，但附带了 Azure 基础设施的其他优势，例如可伸缩性、可用性和隔离性。

可以使用 VNet 预配和管理 Azure 中的虚拟专用网 (VPN)，或者将 VNet 与 Azure 中的其他 VNet 链接，或与本地 IT 基础结构链接，以创建混合或跨云解决方案。 创建的每个 VNet 都有其自己的 地址空间(CIDR)，只要地址空间不重叠，即可链接到其他 VNet 和本地网络。 还可以控制 VNet 的 DNS 服务器设置并将 VNet 分离到子网中。

3.4.2 子网和 IP 地址

使用子网可将虚拟网络划分为一个或多个子网络，并向每个子网分配一部分虚拟网络地址空间。 然后，可以在特定的子网中部署 Azure 资源。 就像在传统网络中一样，使用子网可将 VNet 地址空间划分为适合组织内部网络的网段。 这还会提高地址分配效率。

Azure 的 IP 地址分为专用 IP 地址和公共 IP 地址两类;

专用（或称私有） IP 可在 Azure 中的资源之间进行通信。资源可以是:

- Azure 服务，例如：
- 虚拟机网络接口
- 内部负载均衡器 (ILB)
- 应用程序网关
- 使用 VPN 网关或 ExpressRoute 线路的本地网络。

使用专用 IP，无需使用公共 IP 地址即可与在这些资源之间通信。另外，Azure 从资源所在的虚拟网络子网的地址范围中为资源分配专用 IP 地址，Azure 保留每个子网地址范围中的前四个地址。 不能将这些地址分配给资源，子网的其他地址范围内的 IP 地址一次只能分配给一个资源。地址的分配支持两种选项，一是通过 DHCP 动态分配，这是默认的分配方法。二是手动静态指定分配子网的地址范围内任何未分配或未保留的 IP 地址。

公共 IP 允许 Internet 资源与 Azure 资源进行入站通信。 公共 IP 地址使 Azure 资源能够与 Internet 和面向公众的 Azure 服务进行出站通信。 此地址专门用于该资源，直到你对其取消分配。 无公共 IP 的资源可以进行出站通信。 Azure 会动态分配非专用于该资源的可用 IP 地址，即 NAT 出站。可与公共 IP 地址资源关联的部分资源包括：

- 虚拟机网络接口
- 面向 Internet 的负载均衡器
- VPN 网关
- 应用程序网关
- Azure 防火墙

3.4.3 网络安全组(NSG)

可以使用 Azure 网络安全组来筛选 Azure 虚拟网络中出入 Azure 资源的网络流量。 网络安全组包含安全规则，这些规则可允许或拒绝多种 Azure 资源的入站和出站网络流量。 可以为每项规则指定源和目标、端口以及协议。安全组相当于一个虚拟的四层防火墙，安全组的规则提供以下属性可供配置定义：

属性	说明
名称	网络安全组中的唯一名称。
优先级	介于 100 和 4096 之间的数字。 规则按优先顺序进行处理。先处理编号较小的规则，因为编号越小，优先级越高。一旦流量与某个规则匹配，处理即会停止。 因此，不会处理优先级较低（编号较大）的、其属性与高优先级规则相同的所有规则。
源或目标	可以是任何值，也可以是单个 IP 地址、无类别域际路由 (CIDR) 块（例如 10.0.0.0/24）、服务标记或应用程序安全组。 如果为 Azure 资源指定一个地址，请指定分配给该资源的专用 IP 地址。 在 Azure 针对入站流量将公共 IP 地址转换为专用 IP 地址后，系统会处理网络安全组，然后由 Azure 针对出站流量将专用 IP 地址转换为公共 IP 地址。. 指定范围、服务标记或应用程序安全组可以减少创建的安全规则数。 在一个规则中指定多个单独的 IP 地址和范围（不能指定多个服务标记或应用程序组）的功能称为扩充式安全规则。 只能在通过资源管理器部署模型创建的网络安全组中创建扩充式安全规则。 在通过经典部署模型创建的网络安全组中，不能指定多个 IP 地址和 IP 地址范围。
协议	TCP、UDP、ICMP 或 Any。
方向	该规则是应用到入站还是出站流量。
端口范围	可以指定单个端口或端口范围。 例如，可以指定 80 或 10000-10005。 指定范围可以减少创建的安全规则数。 只能在通过资源管理器部署模型创建的网络安全组中创建扩充式安全规则。 在通过经典部署模型创建的网络安全组中，不能在同一个安全规则中指定多个端口或端口范围。
操作	允许或拒绝

另外，对于安全组的流量安全控制工作原理，可参考：网络安全组 - 工作原理 | Azure Docs

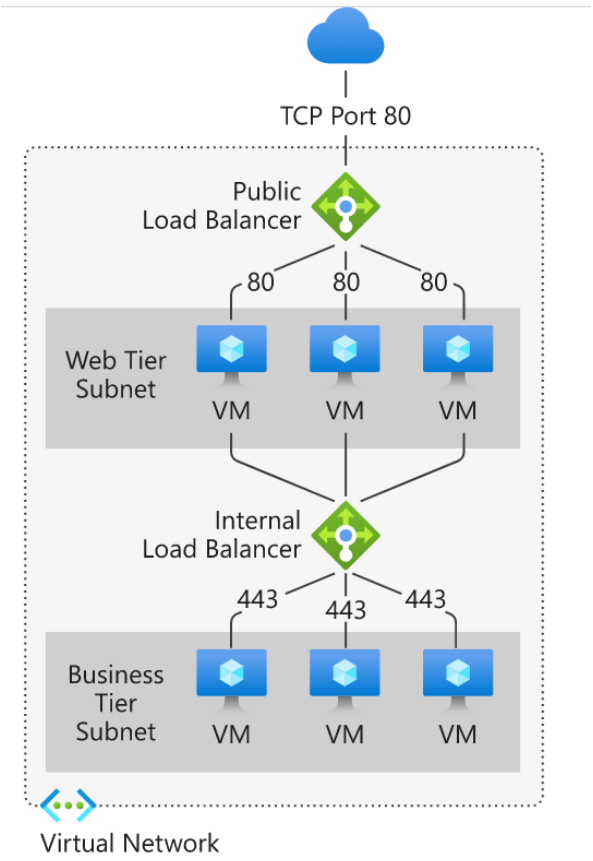
3.4.4 负载均衡&应用程序网关

Azure 负载均衡器在开放式系统互连 (OSI) 模型的第四层上运行。 它是客户端的单一联系点。负载均衡器将抵达负载均衡器前端的入站流量分配到后端池实例。 这些流取决于所配置的负载均衡规则和运行状况探测。 后端池实例可以是 Azure 虚拟机，或虚拟机规模集中的实例。Azure 负载均衡器提供两种 SKU 供选择：

公共负载均衡器 可以为虚拟网络中的虚拟机 (VM) 提供出站连接。 可以通过将专用 IP 地址转换为公共 IP 地址来实现这些连接。 公共负载均衡器用于对传入 VM 的 Internet 流量进行负载均衡。

内部（或专用）负载平衡器 用于仅在前端需要专用 IP 的情况。 内部负载均衡器用于对虚拟网络内部的流量进行负载均衡。 负载均衡器前端可以在混合方案中从本地网络进行访问。

以下是一个通过公共和专用负载均衡器分别在前端接受来自互联网的请求和串接应用的不同组件层的典型架构：

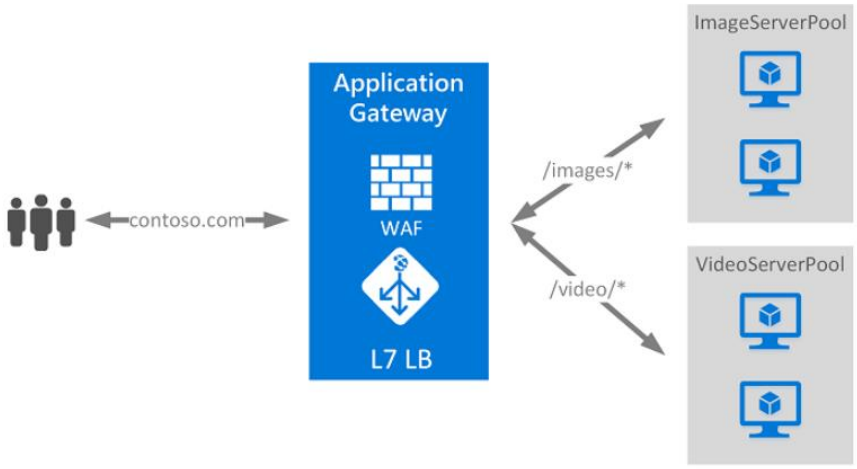


更多关于 Azure 网络负载均衡器的 SKU 差异，组件，轮询算法，运行状态监测等，请参考[负载均衡器 | Azure Docs]

Azure 除了提供基于四层的网络负载均衡，还提供基于七层的 Azure 应用程序网关，应用程序网关是一种 Web 流量负载均衡器，可用于管理 Web 应用程序的流量。并能够根据 HTTP 请求的其他属性（例如 URI 路径或主机头）进行路由决策。

另外，Azure 应用程序网关还提供一键开启 Azure Web 应用程序防火墙 (WAF)的选项， 可以对 Web 应用程序进行集中保护，避免其受到 SQL 注入和跨站点脚本等常见的攻击和漏洞伤害。

最后，举个例子，Azure 应用程序网关是如何基于 URL 路径控制流量导向。例如，可以基于传入 URL 路由流量。 因此，如果 /images 在传入 URL 中，则可将流量路由到为映像配置的一组特定服务器（称为池）中。 如果 /video 在 URL 中，则可将该流量路由到针对视频优化的另一个池中。



需要注意，目前应用程序网关也提供 v1 和 v2 两种 SKU 可供选择，两种 SKU 的功能差异可参考文档[自动缩放和区域冗余应用程序网关 v2 | Azure Docs]

3.4.5 流量管理器

Azure 流量管理器是一种基于 DNS 的流量负载均衡器，可以在 Azure 区域内以最佳方式向服务分发流量，同时提供高可用性和响应性。

流量管理器根据流量路由方法和终结点的运行状况，使用 DNS 将客户端请求定向到最合适的服务终结点。 终结点可以是托管在 Azure 内部、本地或其他云平台的任何面向 Internet 的服务。流量管理器提供多种流量路由方法和终结点监视选项来满足不同的应用程序需求和自动故障转移模型。 流量管理器能够帮助用户灵活应对故障，包括整个 Azure 区域的故障。通过流量管理器，可以获得以下价值：

- 提高应用程序可用性
- 改善应用程序性能
- 在无需停机的情况下维护服务的某一节点
- 与分布在不同环境的基础架构进行切换或弹性扩展
- 利用流量管理器配置文件调度操控复杂的流量调度

关于流量管理器所支持的流量调度方法，请参考 [Azure 中的嵌套式流量管理器配置文件 - Azure Traffic Manager | Azure Docs]

3.4.6 内容加速 CDN

Azure CDN （内容传送网络） 通过遍布在中国大陆的众多物理节点上缓存 Azure 平台上的 Storage Blob，Cloud Service 和 WebSites 的静态内容，以及为媒体服务提供流式内容分发提供加

速。Azure China 的 CDN 服务是融合 CDN，在国内覆盖范围广，与 Azure 服务深度集成，并具有以下优势：

- 默认对包括 Cloud Service，Storage Blob，Web App，Media service,媒体服务等在内的多种 Azure 服务的原生支持，为用户提供完整的一站式云服务支持。
- 传统的 CDN 服务需要很多复杂冗长的配置流程。对于 Azure CDN 用户来说，从创建 CDN 加速节点，到之后的对 CDN 加速节点整个生命周期的管理，以及各种统计报表的查询，原始访问日志下载，各种高级功能（如缓存规则配置，缓存内容强制刷新，内容预加载，防盗链等）的配置，均可以通过 Azure 管理门户以及专门的 CDN 管理门户自助完成。
- 整合国内多家主流 CDN 服务，提供全面的静态网页加速，软件安装包、游戏客户端、应用程序、影音等大文件的下载分发，以及在线视频网站、在线教育网站等以流媒体为主的视频点播和直播等多种业务类型加速，满足不同类型资源的分发需求；提供包含电信、联通、移动等主流电信运营商，以及其他 ISP 运营商，全地区的全网覆盖，根据网络实时状况，通过负载均衡技术和智能调度策略，将用户请求分配到最优节点。
- 依托和多家主流 CDN 服务的合作优势，Azure CDN 可以给包括企业客户，网站支付用户在内的所有 Azure 用户，提供质优价廉的 CDN 服务。让更多的用户可以享受到 CDN 服务所带来的红利。
- 另外，利用丰富的海外节点，Mooncake 的 CDN 服务同时支持海外加速，通过智能调度系统进行精准调度，提供静态、下载、点播等多种加速业务，为您的出海访问提供优质的全球网络服务。
  Azure CDN 的节点分布情况，可参考：Azure CDN POP - Azure feature guide | Azure Docs

3.4.7 用户自定义路由

Azure 默认自动为 Azure 虚拟网络中的每个子网创建一个路由表，并将路由分配到虚拟网络中的每个子网。 你不能创建系统路由，也不能删除系统路由，流量转发都需要根据默认路由表表项进行，但对于某些需求，用户需要按照实际需求修改路由转发规则，例如，在 azure 网络部署 NVA 设备，所有 vnet 内网络流量都需要先转发到 NVA 设备，再通过 NVA 设备根据指定的规则转发到下一跳，这时 Azure 提供了用户自定义路由的功能来满足这类型场景的需求。

创建用户定义（静态）路由，可以替代 Azure 的默认系统路由，或者向子网的路由表添加其他路由。 在 Azure 中创建一个路由表后，将该路由表关联到虚拟网络子网。 每个子网可以有一个与之关联的路由表，也可以没有。用户自定义路由表可以使用以下选项作为其路由的下一跳目标：

- NVA 虚拟设备，例如，第三方的虚拟路由器、防火墙
- 虚拟网络网关（VPN 网关）
- 虚拟网络：需要替代该虚拟网络的默认路由时才选择此选项
- 无：作为黑洞路由时选择此选项

3.4.8 访问互联网方式

默认情况下，VNet 中的所有资源都可以与 Internet 进行出站通信。 可以通过分配公共 IP 地址或公共负载均衡器、Azure 防火墙等进行入站通信。 还可以使用公共 IP 或公共负载均衡器、Azure 防火墙来管理出站连接。

通过负载均衡出向 NAT 可参考：使用 Azure 负载均衡器配置出站规则 | Azure Docs

通过 Azure 防火墙出向访问 Internet 可参考：Azure 防火墙功能 | Azure Docs

3.4.9 连接本地数据中心/网络

Azure 提供 VPN 或 Expressroute 上云专线两种连接方式连接 Azure 虚拟网络与本地数据中心、办公网络或个人终端。

VPN 连接用于跨公共 Internet 在 Azure 虚拟网络和本地位置之间发送加密的流量。 VPN 连接需要本地网络边界提供对接设备与 Azure VPN 网关进行对接，建立 IPSec 隧道；每个虚拟网络只能有一个 VPN 网关，但是，可以创建连接到相同 VPN 网关的多个连接。 与同一个 VPN 网关建立多个连接时，所有 VPN 隧道共享可用的网关带宽。另外，对于个人终端连接 Azure 虚拟网络可以通过终端与 Azure 虚拟网关建立点到站点的 SSLVPN 连接隧道。Azure 提供多个规格的 VPN 网关，不同规格网关所支持的性能如下：

SKU	S2S/VNet 到 VNet 隧道	P2S SSTP 连接	P2S IKEv2/OpenVPN 连接	聚合吞吐量基准	BGP
基本	最大 10 个	最大 128	不支持	100 Mbps	不支持
VpnGw1	最大 30*	最大 128	最大 250	650 Mbps	支持
VpnGw2	最大 30*	最大 128	最大 500	1 Gbps	支持
VpnGw3	最大 30*	最大 128	最大 1000	1.25 Gbps	支持

与 Azure VPN 网关建立 IPSec vpn 可参考：将本地网络连接到 Azure 虚拟网络：站点到站点 VPN：门户 - Azure VPN Gateway | Azure Docs

与 Azure VPN 网关建立 SSL vpn 可参考：使用 P2S VPN 和证书身份验证连接到 VNet：门户 - Azure VPN Gateway | Azure Docs

建立 SSL VPN 除了可以使用基于证书的身份验证或 RADIUS 身份验证。 在使用开放 VPN 协议时，还可以使用 Azure Active Directory 身份验证。

对于需要与本地数据中心有长期稳定且吞吐较大的数据交往时，可以考虑使用速度更高，稳定性更好的 azure expressroute 专线服务，详细信息可参考：ExpressRoute 文档 | Azure Docs

3.4.10 Azure 虚拟网络/资源之间通信

在 Azure 内虚拟网络之间建立连接，供虚拟网络内资源间建立通信和流量转发的场景，Azure 提供了两种实现的选项，一是可以将两个网络看作本地网络，通过在网络边界建立 VPN 网关，网关之间建立 IPSec VPN 隧道；二是使用 Azure 虚拟网络提供的虚拟网络对等互连功能，这也是 Azure 更为推荐的方式。以下简单介绍一下虚拟网络对等互连的优势:

- 不同虚拟网络中资源之间的连接延迟低且带宽高。
- 一个虚拟网络中的资源可与另一个虚拟网络中的资源通信。
- 可以在跨 Azure 订阅、Azure Active Directory 租户、部署模型和 Azure 区域的虚拟网络之间传输数据。
- 可以对等互连通过 Azure 资源管理器创建的虚拟网络。
- 可将通过资源管理器创建的虚拟网络对等互连到通过经典部署模型创建的虚拟网络。
- 在创建对等互连之时或之后，虚拟网络中的资源不会出现停机的现象。
- 对等虚拟网络之间的网络流量是专用的。 虚拟网络之间的流量仅限于 Azure 主干网络。 在虚拟网络之间通信不需公共 Internet、网关或加密。

同一区域中对等互连虚拟网络上的虚拟机之间的网络延迟与单个虚拟网络中的延迟相同。 网络吞吐量取决于可供虚拟机使用的与其大小成比例的带宽。 对等互连的带宽没有任何其他限制。

对于使用虚拟网络对等互连的要求和限制，请参考：创建、更改或删除 Azure 虚拟网络对等互连 | Azure Docs

3.4.11 Azure 网络基础服务 SLA

本章节提及到的 Azure 网络基础服务 SLA 可参考以下对应文档说明:

- 负载均衡器: 负载均衡器 (azure.cn)
- 应用程序网关: 应用程序网关 (azure.cn)
- VPN 网关: VPN 网关 (azure.cn)
- CDN: CDN (azure.cn)
- 流量管理器: 流量管理器 (azure.cn)
- Expressroute: ExpressRoute (azure.cn)
- Azure 防火墙: Azure 防火墙

4. 创建 Azure 虚拟机实验环境

4.1 模拟实验场景概述

Contoso 公司最近采购了 Azure 服务，计划把现有托管在 IDC 的企业官网迁移到 Azure 云平台。该企业官网面向的用户群主要是华东地区的用户。

该企业官网部署需要服务器列表如下：

1. 2 台 AD 服务器在一个可用性集。
2. 2 台 Web 服务器在一个可用性集。
3. 2 台 SQL Server 服务器在一个可用性集。
4. 2 个负载均衡器分别用于前端 Web 服务器和后端 SQL Server。
5. 为全部机器规划高可用，我们在创建虚拟机的时候同时创建**可用性集**即可。

注：在后面的章节里将详细介绍创建过程。

4.2 规划要点

4.2.1 如何选择 Azure 数据中心

世纪互联运维的微软 Azure 在中国大陆有四个数据中心:

- 中国北部 1 和中国北部 2 位于北京的数据中心。
- 中国东部 1 和中国东部 2 位于上海的数据中心。

附：Azure 地域地图

https://azure.microsoft.com/zh-cn/global-infrastructure/geographies/

当我们在选择 Azure 数据中心的时候，需要从以下三方面进行考虑：

1. **选择的 Azure 数据中心离最终用户越近越好**
   考虑到 Contoso 的企业官网主要的用户群是华东地区，建议 Contoso 公司将应用部署到 Azure 在中国东部的数据中心。

2. **如果需要在 Azure 部署多台应用服务器，则需要将所有的应用服务器放在同一个**

数据中心
建议用户将 Web 服务器和 SQL Server 服务器都部署在 Azure 中国东部数据中心，不要将 Web 服务器和 SQL 服务器部署在不同的数据中心，会产生内部通信的延时。

3. **利用 CDN**
CDN 能将静态内容缓存到离用户最近的 CDN 节点服务器，提高应用程序的用户体验。
https://www.azure.cn/home/features/cdn/

4.2.2 选择最合适的虚拟机配置

传统的虚拟机化技术的 CPU 是和其他资源共享的，如 VMware 的宿主机和虚拟机实例共享其物理 CPU。Azure 虚拟机老的机型 vCPU 是独占物理 CPU 分配给用户的。Dv3，Ev3 引入超线程，vCPU 代表的是一个 CPU 线程。

如第 4.4.2 章，常用 Azure 虚拟机有 D 系列和 F 系等，并且拥有不同的 CPU 和内存配置。

如果客户在传统 IDC 托管中已经部署了硬件服务器。则在 Azure 平台选择最接近的 Azure 虚拟机配置即可。

如果客户需要部署新的应用，则需要根据并发、性能等多个因素，选择最合适的 Azure 虚拟机配置。

举一个例子说明 D 系列虚拟机和 F 系列虚拟机的计算力区别：

1. D 系列虚拟机单台最大的配置为 20 Cores/140GB RAM (D15 v2) 。F 系列虚拟机单台最大的配置为 72 Cores/144GB RAM (D15 v2) 。
2. F 系列的 CPU 性能比 D 系列提升约 350%。

其他内容，请参考第 4.4.2 章或者登录：

https://www.azure.cn/pricing/details/virtual-machines.html

4.2.3 规划好高可用

在 Microsoft Azure 虚拟机中，用户可以选择使用一台 Azure Virtual Machine 部署 AD Server，一台 Azure Virtual Machine 部署 Web Application，使用另一台 Virtual Machine 部署 SQL Server。这些场景均提供相应的 SLA（服务级别协议）保障。详细请参阅章节 **3.1.6**。

对于本场景:

1. 在同一可用性集的两台 AD Server 中的内容配置必须完全一致，并且需要进行 AD 的同步。
2. 在同一可用性集的两台 Web Server 中的网站在部署的时候，内容必须完全一致。
3. 在同一可用性集的两台 SQL Server 必须配置 SQL Server Always-On 或者 SQL Mirroring，保证数据库之间的日志同步。
4. 对于 DB Server，比如 SQL Server 或者 MySQL，需要在两台 DB Server 进行日志同步:
   - SQL Server 需要在两台 VM 配置 Always-On 或者 SQL Mirroring，使用日志同步
   - My SQL 可以配置 Master-Slave，使用 Replication 进行复制。
   - 这样的目的是保证在其中一台 Server 宕机的情况下，另外一台 Server 可以正常运行，因为配置了日志同步，可以保证日志不会丢。
   - 另外还要强调一下，客户端如果调用 SQL Server 服务的时候，需要正确配置 AG Listener，这样保证在一台 SQL Server 宕机的情况下，AG Listener 可以将请求自动发送到另外一台 SQL Server 上。

4.2.4 规划好 Azure 订阅

订阅是进行 Azure 账单分拆的最小单位。如果企业内部需要进行内部成本核算，例如 IT 部门、销售部门、市场部门均需要使用 Azure，并且根据不同的部门的 Azure 实际使用量进行内部成本核算，就需要实现规划好不同的 Azure 订阅。在创建 Azure IaaS 相关资源的时候，将这些资源创建在不同的订阅下。

如果你的组织有多个订阅，则可能需要一种方法来高效地管理这些订阅的访问权限、策略和符合性。 Azure 管理组提供订阅上的作用域级别。 可将订阅组织到名为“管理组”的容器中，并将管理条件应用到管理组。 管理组中的所有订阅都将自动继承应用于管理组的条件。 不管使用什么类型的订阅，管理组都能提供大规模的企业级管理。 单个管理组中的所有订阅都必须信任同一个 Azure Active Directory 租户。

例如，可将策略应用到限制创建虚拟机 (VM) 的区域的管理组。 此策略将应用到该管理组下面的所有管理组、订阅和资源，只允许在该区域中创建 VM。

https://docs.azure.cn/zh-cn/governance/management-groups/overview

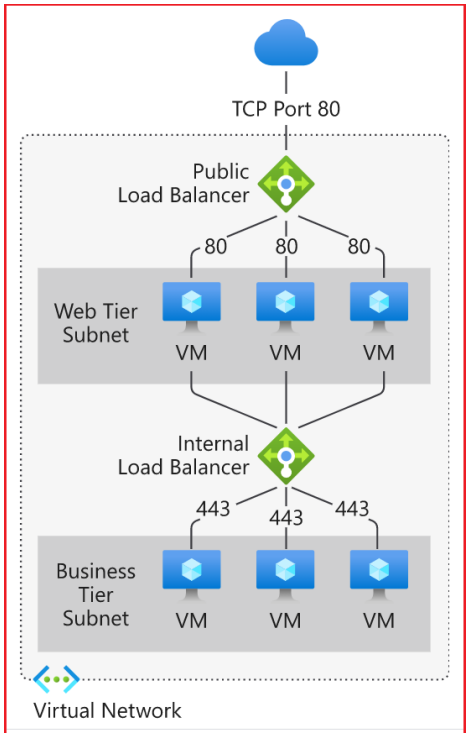
4.2.5 Azure 是如何解决并发问题的?

我们建议使用多台 Azure 虚拟机并利用横向扩展的方式来解决大量的并发。受限于现有的 CPU 制造技术，单个节点向上扩展是有限的。比如我们无法将大量的计算资源都堆

积到 1 台 300 Core 甚至 400 Core 的计算节点上。对于需要大量的计算资源的情况下，我们可以通过横向扩展的方法来解决。

横向扩展就是由 1 个计算节点，横向扩展到多个计算节点上并行计算，比如 50 个、100 个计算节点。比如一个互联网业务需要大量的计算资源，那可以将这些计算需求由 100 台 4 Core 的计算节点进行并行计算。

如下图：



4.2.6 查看该订阅中可使用的 Azure 资源

如果您使用的是企业试用账号，只能有一个订阅，该订阅默认情况下可以使用的 Azure 资源为:

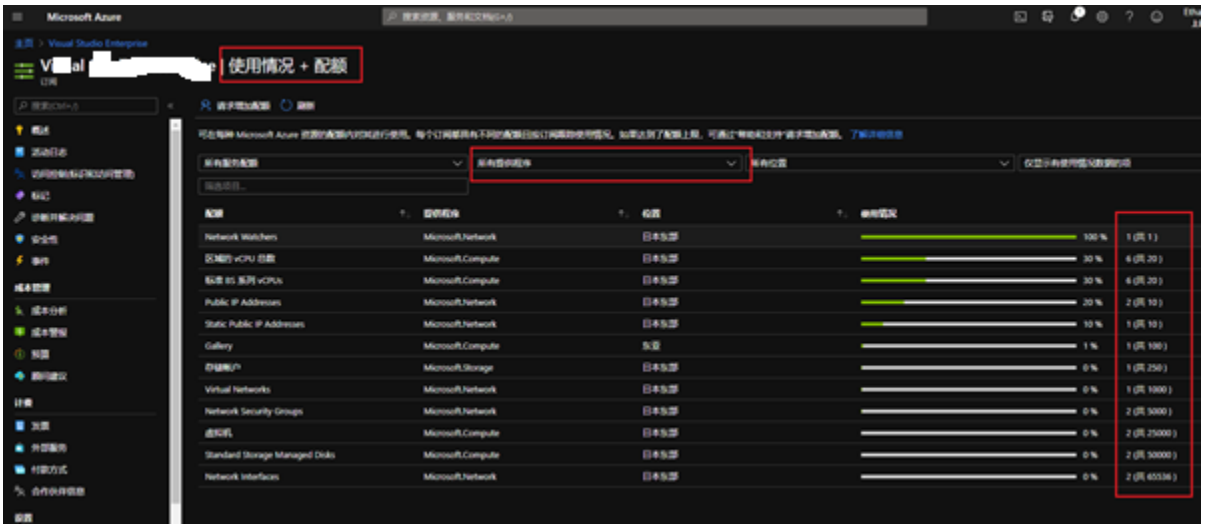
1. 每个测试账号的额度默认设定为 3500 元（Azure 中国企业试用）.
2. 每个账号的有效时间为 3 个月 (120 天)，账号会在到期后自动关闭.
3. 此测试账号一般无法进行延期和充值，如需大量开发测试，请用户自行采购进行开发测试。

如果您使用的是正式账户，可以创建无限多个订阅。新创建的 Azure 订阅默认可以使用的 Azure 资源为:

1. 虚拟机：每个订阅在所有区域最多可部署 20 vCPUs。
2. 存储服务：每个订阅在所有区域最多可部署 200 个。
3. 数据传输：我们为您提供免费的入站数据传输服务。
4. Active Directory：150,000 个对象
5. 服务级别协议 (SLA)：我们为每个公开发布的 Azure 平台服务提供一套可靠的服务级别协议 (SLA)。

如果正式账户在使用过程中需要的 Azure 资源超出订阅默认的 Azure 资源，请直接联系世纪互联支持团队 Azure 在线支持（通过”帮助+支持”，提交“配额申请”分类的请求），世纪互联会先审核相关请求，然后会将该订阅的相关资源进行扩大。

我们登陆 Azure 管理界面，点击订阅中的**“使用情况+配额”**查看该订阅的资源情况：



4.3 创建虚拟实验环境

4.3.1 环境搭建详细说明

本实验例子意在快速入门，具体设置会因实际为准。首先需要对 Azure 虚拟机进行环境配置，主要分为：

1. 选择虚拟机的操作系统及配置。
2. 两个负载均衡器，分为前端 WEB 服务和后端 SQL。前端通过公共负载均衡与用户链接，后端 SQL 通过内部负载均衡与前端连接。内部负载均衡可以有效提升数据安全，即外部用户无法直接访问后端 SQL 虚拟机。
3. 数据中心选择中国东部 2。

4. 创建虚拟网络，规划虚拟机的内网 IP 地址和 IP Range：
   - 我们创建 Azure 虚拟网络，命名为 **ContosoVNet**，同时设置虚拟网络的 IP Rang 为 **10.1.0.0 - 10.1.3.255**
   - 设置 3 个 Sub-net
     - **AD-Subnet，IP Rang 为– 10.1.0.255**
     - **Web-Subnet，IP Rang 为 10.1.1.0 – 10.0.1.255**
     - **DB-Subnet，IP Rang 为 10.1.2.0 – 10.0.2.255**

请看以下表格：

角色	AD Server	Web Server	DB Server
操作系统	Server 2019	Server 2019	SQL Server 2019 Enterprise on Win server 2019
虚拟机类型	F 系列	F 系列	F 系列
虚拟机数量	2 台	2 台	2 台
虚拟机名称	ContosoAD01 ContosoAD02	ContosoWeb01 ContosoWeb02	ContosoDB01 ContosoDB02
虚拟网络子网	AD-Subnet	Web-Subnet	DB-Subnet
内网 IP	10.1.0.4 10.1.0.5	10.1.1.4 10.1.1.5	10.1.2.4 10.1.2.5
可用性集	ADAvbSet	WebAvbSet	DBAvbSet

4.3.2 创建虚拟网络

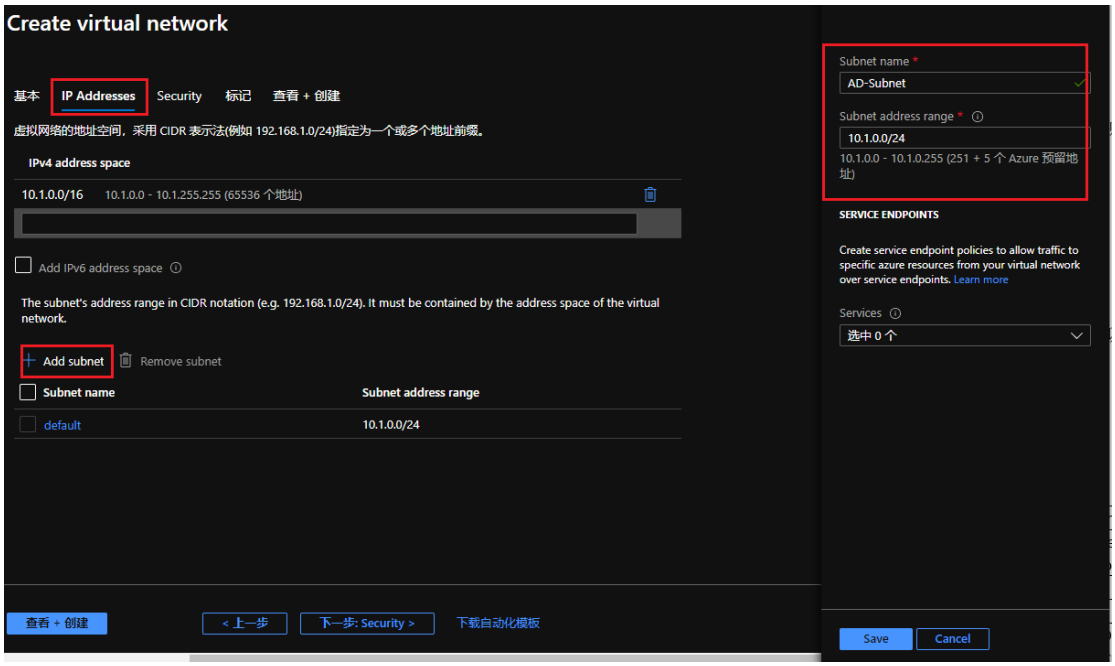
下面我们开始创建本实验所需的虚拟网络

登陆 Azure 管理界面 https://portal.azure.cn，输入相应的 Azure 账户名称和密码。

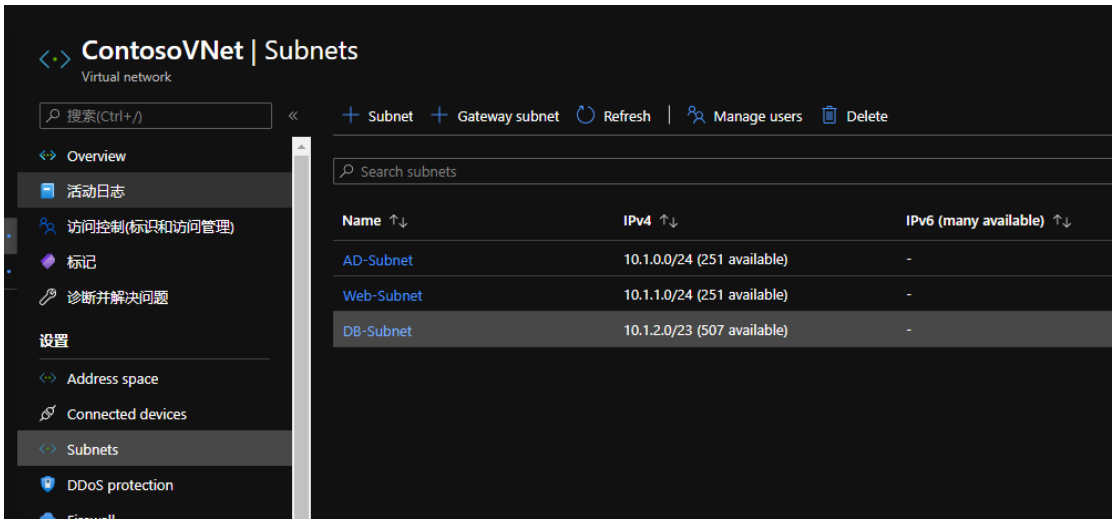
1. 搜索**“虚拟网络”**在 Azure 管理界面的左下角，点击**“+”**按钮：

2. 在弹出的窗口中，将名称命名为 **ContosoVNet**，位置我们选择“中国东部 2”：

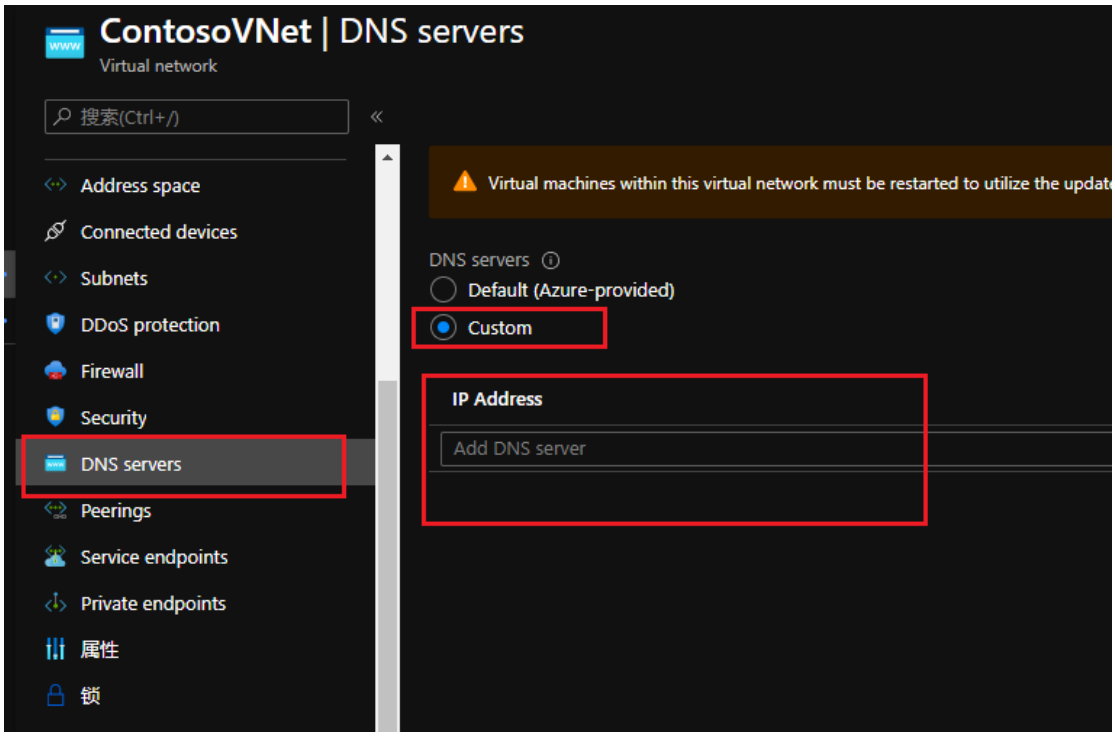
3. 参考以下步骤分别创建三个子网，如下图：



检查一次确保无误，如图：

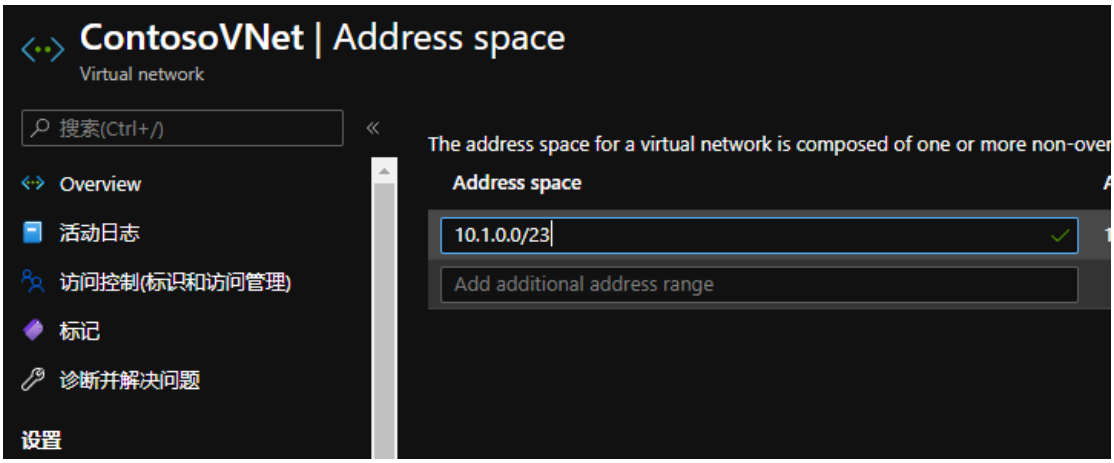


4. DNS 需要在后期 AD server 建立好之后在 **“DNS”** 里设置。

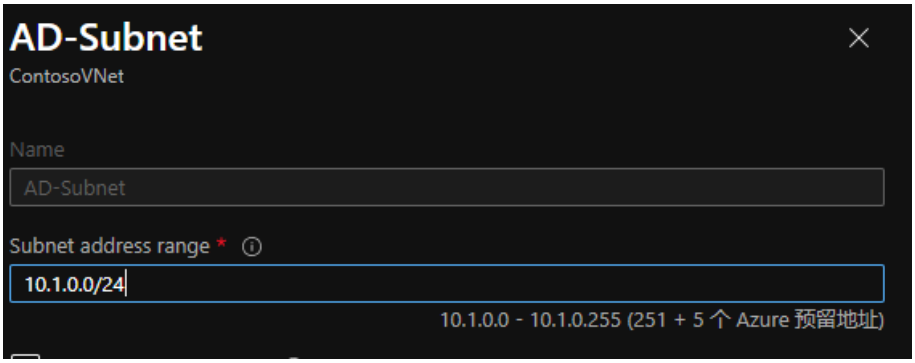


5. 最后，我们整理一下虚拟网络的详细情况后继续试验。

(1) 整个虚拟网络的 IP Range 为 10.1.0.0-10.1.3.255



(2) 子网 AD-Subnet 的 IP Range 为 **10.1.0.0-10.1.0.255**。注意每个子网的 5 个 IP 是 Azure **系统保留的(0-3 以及 255 不可用)**，对于 AD-Subnet 来说，可用的 IP Range 为 **10.1.0.4-10.1.0.254**。



(3) 同理,子网 **Web-Subnet** 的 IP Range 为 10.1.1.0 – 10.1.1.255。该子网实际可用的 IP Range 为 **10.1.1.4-10.1.1.254**。

(4) 同理,子网 **DB-Subnet** 的 IP Rang 为 10.1.2.0 – 10.1.3.255。该子网的实际可用 IP Range 为 **10.1.2.4-10.1.3.254**。

在 Azure 云平台 vNet 会自带 DHCP。举个例子如果我们将第一台虚拟机 VM01，通过管理界面进行创建，加入到 AD-Subnet 的话，这台虚拟机 VM01 会自动获得第一个可用的内网 IP (Private IP)，为 10.1.0.4。

如果我们在第一台虚拟机 VM01 不关机的情况下。再次通过管理界面继续创建第 2 台虚拟机 VM02，同样加入到 AD-Subnet。因为 10.0.0.4 这个 IP 被第一台虚拟机 VM01 占用。所以第 2 台虚拟机 VM02 自动获得下一个可用的内网 IP 地址，为 10.1.0.5。如果 VM01, VM02 都不关机的情况下（关机 IP 地址会被释放），则第 3 台新创建的虚拟机 VM03 加入到 AD-Subnet 的 Azure 虚拟机自动获得下一个可用的内网 IP 地址为 10.1.0.6。

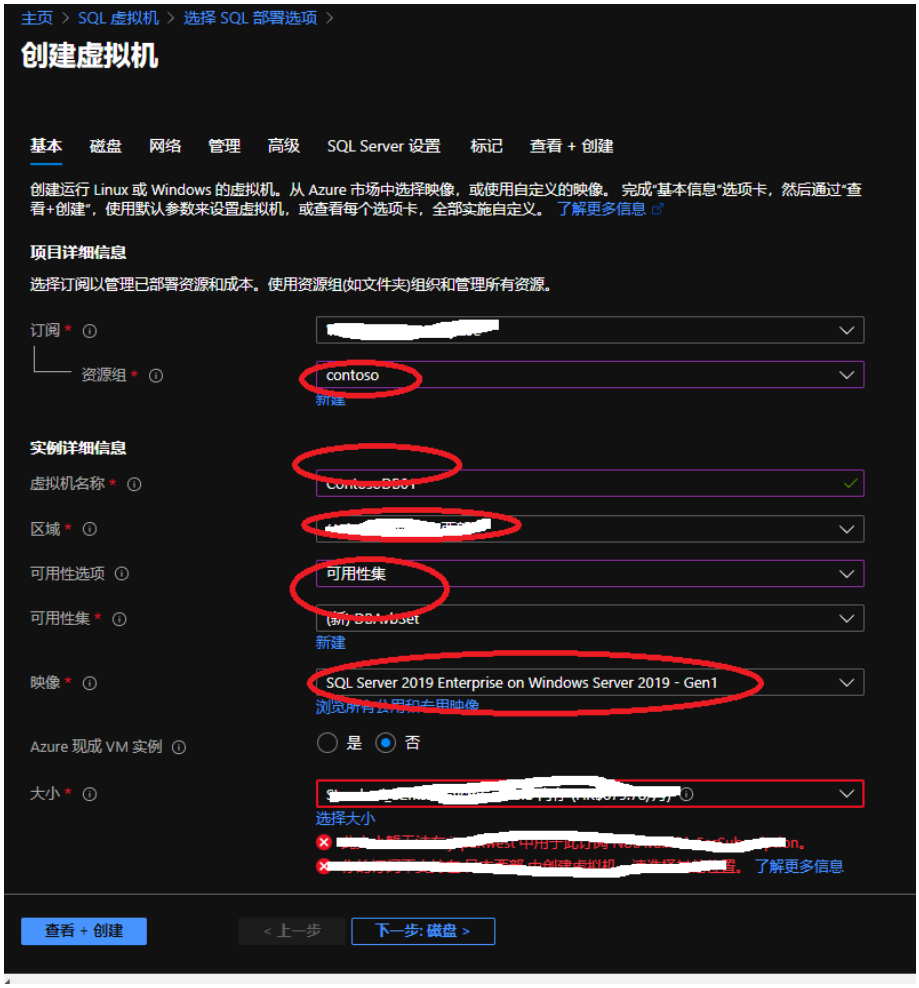
4.3.3 创建 Azure 虚拟机

4.3.3.1 创建 AD Server

根据我们在 5.3.2 节的规划，我们需要创建 2 台 Azure AD Server，配置如下：

角色	AD Server
操作系统	Server 2019
虚拟机类型	F 系列
虚拟机名称	ContosoAD01 和 ContosoAD02
虚拟网络子网	AD-Subnet
默认内网 IP	10.1.0.4/10.1.0.5
可用性集	ADAvbSet

1. 我们登陆 Azure 管理界面 https://portal.azure.cn。搜索**“虚拟机”**然后点击**“+”**，按照以下配置创建名 **ContosoAD01** 的 VM。在创建虚拟机同时创建高可用，如图：



2. 以下是虚拟网络的配置信息：

3. 最后我们点击确认，这样就完成创建第一台 AD Server。
4. 我们随后用同样的方法创建第 2 台 AD Server ContosoAD02 并将其加入同一个高**可用性集 ADAvbSet** 里。
5. 我们等待第 2 台虚拟机创建完毕，状态变为"正在运行"。然后我们观察一下 Azure 管理界面。

4.3.3.2 创建 Web Server

创建 2 台 Web Server，配置信息如下：

角色	Web Server
操作系统	Server 2019
虚拟机类型	F 系列
虚拟机名称	ContosoWeb01 和 ContosoWeb02

虚拟网络子网	Web-Subnet
默认内网 IP	10.1.1.4/10.1.1.5
可用性集	WebAvbSet

1. 我们在创建两台 Web Server 的时候需要选择对应的虚拟网络并注意子网为 **Web-Subnet**。
2. 同时选择我们之前已经创建的可用性集 **WebAvbSet**。

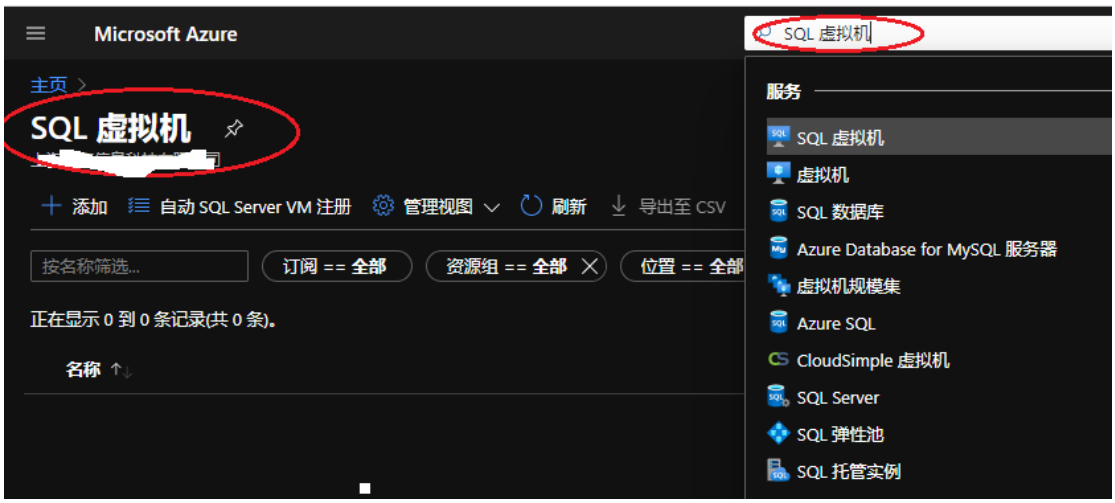
4.3.3.3 创建 SQL Server 虚拟机 创建 SQL Server

创建两台 SQL Server，配置信息如下:

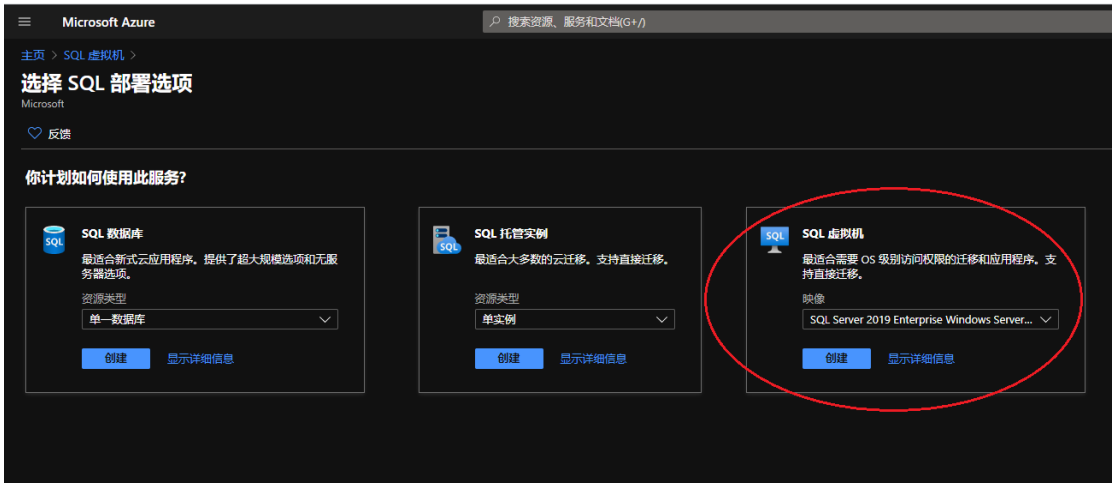
角色	DB Server
操作系统	SQL Server 2019 Enterprise on Windows server 2019
虚拟机类型	F 系列
虚拟机数量	2 台
虚拟机名称	ContosoDB01 和 ContosoDB02
虚拟网络子网	DB-Subnet
默认内网 IP	10.1.2.4/10.1.2.5
可用性集	**DBAvbSet**

创建 **SQL 虚拟机**和创建普通虚拟机有不同，具体如下:

搜索“SQL 虚拟机”,然后点添加，根据上表给出的信息创建两台 SQL 虚拟机:



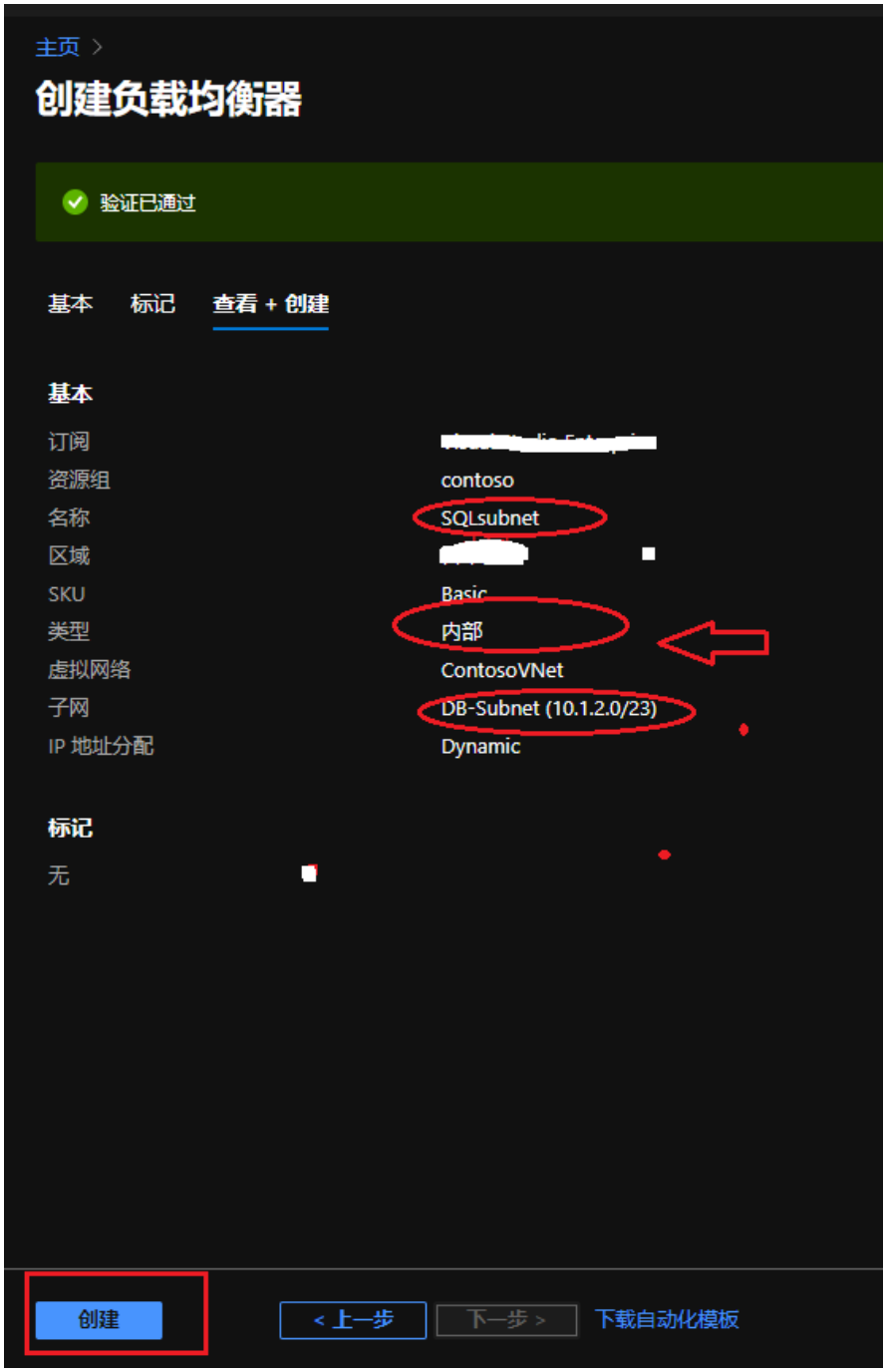
在本实例中我们选择 **SQL 虚拟机**。
如果我们不需要管理操作系统我们可以选择“SQL 数据库” 或者 “SQL 托管实例“。



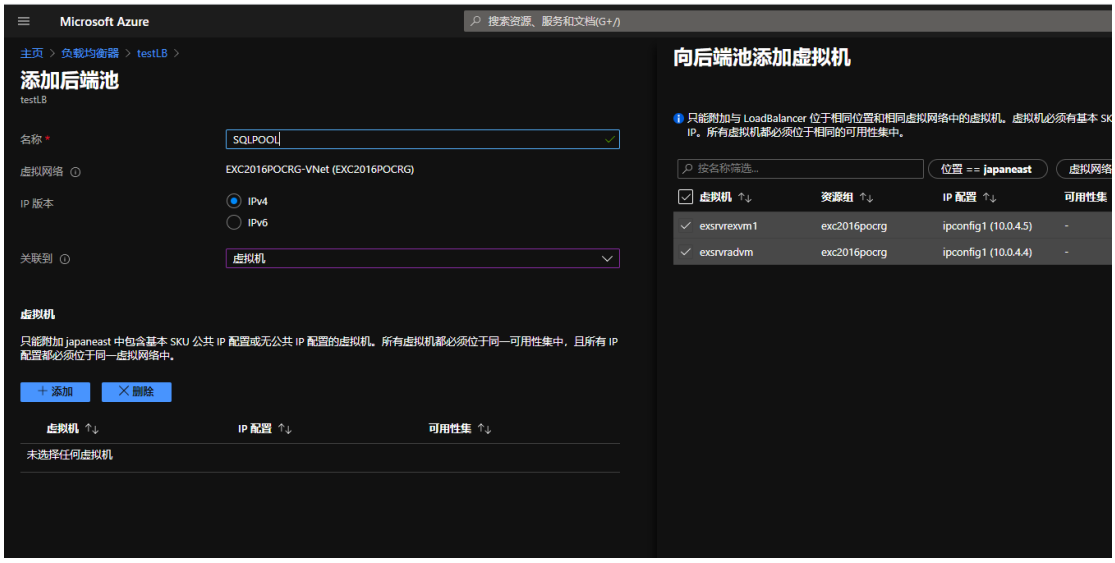
4.3.4 配置负载均衡

我们可以把虚拟机加到负载均衡里。分两部分：

1. 我们建议把两台 SQL 服务器加到第一个负载均衡里。由于 SQL 服务器在**后端**，出于数据安全我们是用**内部负载均衡器**。 内部负载均衡器用于对虚拟网络内部的流量进行负载均衡。 负载均衡器前端可以在混合方案中从本地网络进行访问。创建时记得**复用相应的虚拟机网络**保证其互通性：



把两台 SQL 服务器加到内部负载均衡器：



（图片为例子，请忽视虚拟机名字，主要是说明如何添加虚拟机到后端池。）

2. 我们建议把两台 **WEB 服务器**加到第二个负载均衡里，由于 WEB 在前端，选用**公共负载均衡器**可以为虚拟网络中的虚拟机 (VM) 提供出站连接。 可以通过将专用 IP 地址转换为公共 IP 地址来实现这些连接。 公共负载均衡器用于对传入 VM 的 Internet 流量进行负载均衡，配置与上述类同。

附负载均衡主题包含内部/外部负载均衡的图谱图，请参阅：

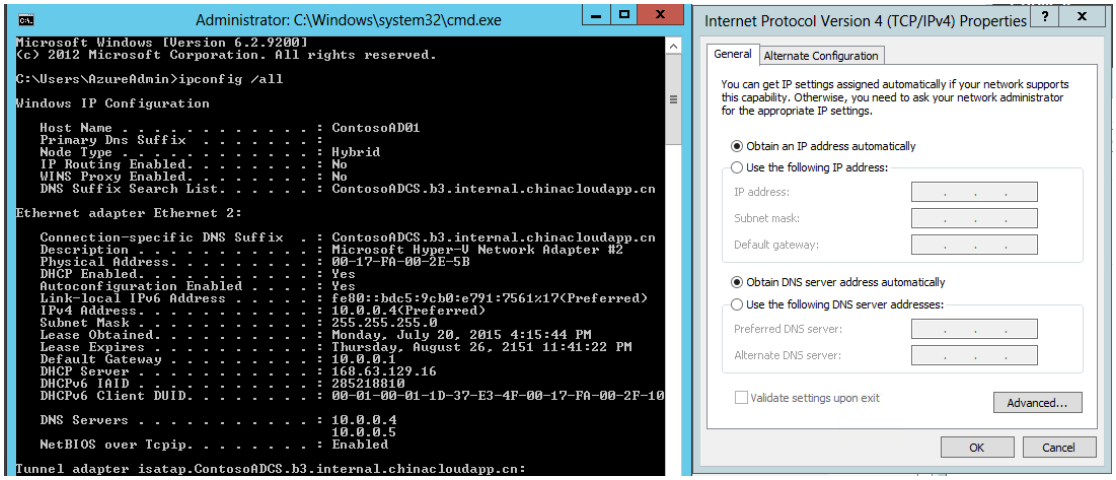
https://docs.azure.cn/zh-cn/load-balancer/load-balancer-overview

4.4 管理 Azure 虚拟机

4.4.1 远程桌面连接 Windows VM

- 我们选中其中一个在之前创建成功的 ContosoAD01 这台虚拟机。

- 点击图中的“链接”即可下载 RDP 文件，链接到此虚拟机。
- 系统会提示输入相应的用户名和密码进行登陆。
- 我们就可以通过远程桌面连接，在这台 Azure **虚拟机上安装和配置功能和角色**。
- 我们在 ContosoAD01 这台虚拟机上，通过 CMD 执行 ipconfig /all 命令，可以看到如下信息：



虽然 ContosoAD01 这台虚拟机的 TCP/IPv4 的属性是自动获取，但是在 ipconfig 命令中，看到的 DNS 服务器是 10.1.0.4 和 10.1.0.5，这 2 个地址，恰恰是我们在 Azure 虚拟网络中预先设置好的。在 Azure 云环境，Azure 虚拟机的 Private IP，DNS Server 都必须通过虚拟网络来设置。我们不可以通过远程桌面连接(Remote Desktop)，来修改 Azure 虚拟机的本地 TCP/IP 地址。如果这样操作的话，Azure 虚拟机会运行不正常。

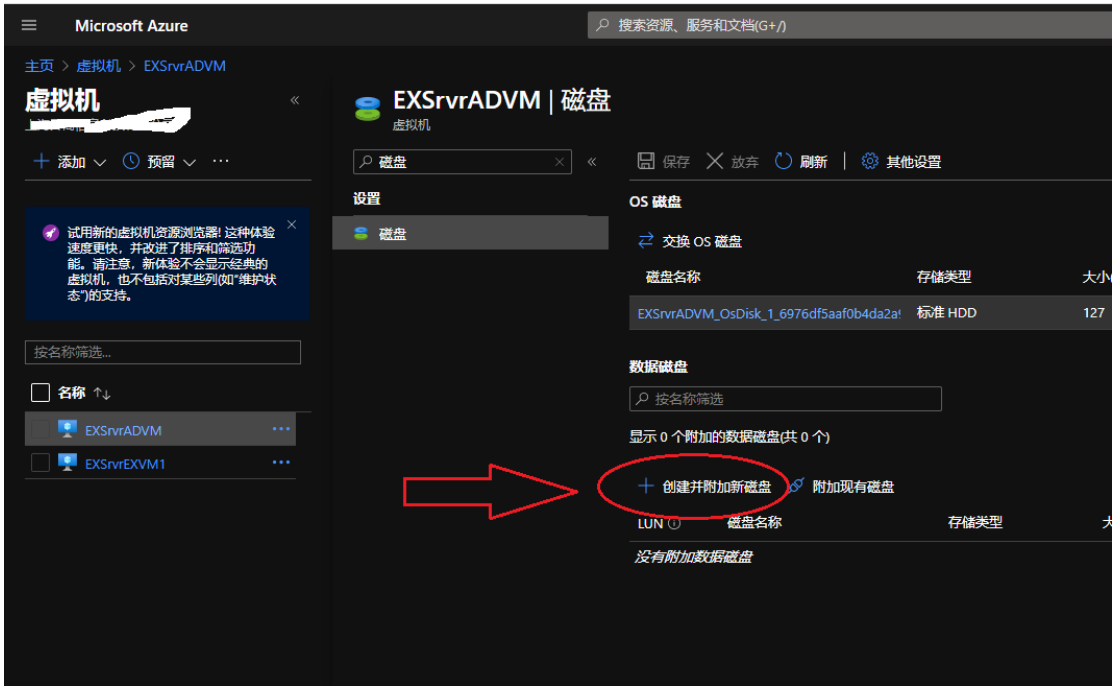
登录并配置 WebServer 和 SQLServer 并配置 SQLserver 的复制，这里不再赘述。

4.4.2 挂载磁盘

在 Windows 平台，Azure 虚拟机默认有两块磁盘：

1. C 盘，操作系统盘，默认为 127GB
2. D 盘，临时磁盘。只能用来保存临时文件，数据会有丢失的风险。

假设我们要挂载更多的磁盘：



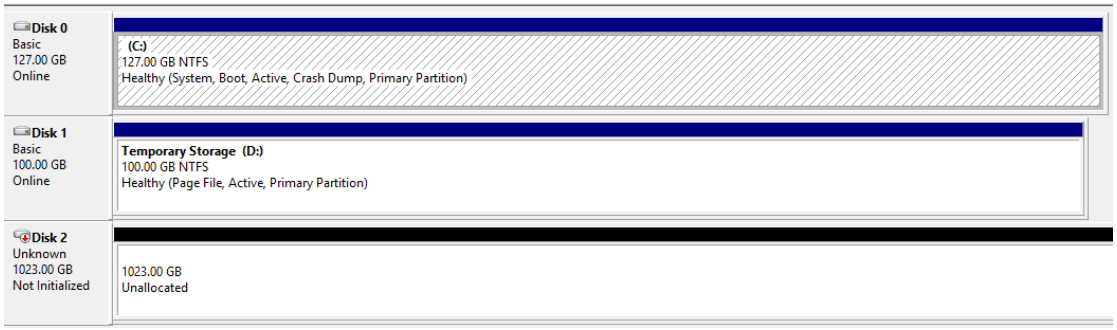
https://docs.azure.cn/zh-cn/virtual-machines/windows/attach-managed-disk-portal

注意：LinuxVM 添加方式有所不同，除了在 Azure 平台添加，某些 Linux 版本，需要在添加后在 Linux 系统内更新文件系统：

使用门户将数据磁盘附加到 Linux VM：

https://docs.azure.cn/zh-cn/virtual-machines/linux/add-disk

磁盘挂载完毕后，我们通过远程桌面连接，计算管理中的磁盘管理，来重新格式化和分配相应的磁盘空间，如下图：

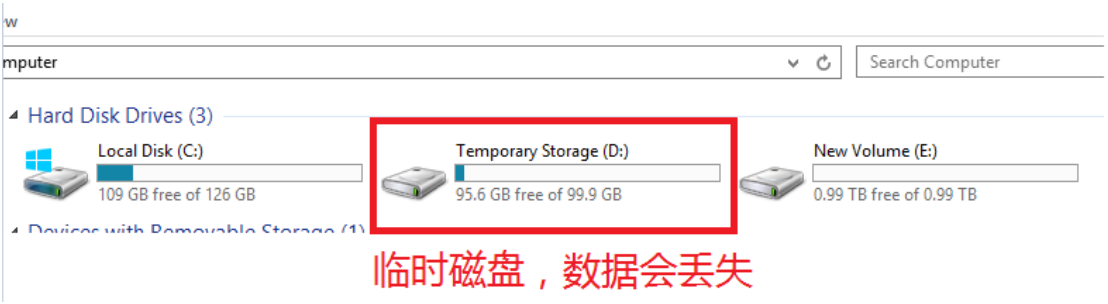


不同的虚拟机尺寸可以挂载的磁盘数目不同如：

Size	vCore	Memory: GiB	Temp storage (SSD) GiB	Max temp storage throughput: IOPS/Read MBps/Write MBps	Max data disks/throughput: IOPS	Max NICs	Expected network bandwidth (Mbps)
Standard_A1_v2	1	2	10	1000/20/10	2/2x500	2	250
Standard_A2_v2	2	4	20	2000/40/20	4/4x500	2	500
Standard_A4_v2	4	8	40	4000/80/40	8/8x500	4	1000
Standard_A8_v2	8	16	80	8000/160/80	16/16x500	8	2000
Standard_A2m_v2	2	16	20	2000/40/20	4/4x500	2	500
Standard_A4m_v2	4	32	40	4000/80/40	8/8x500	4	1000
Standard_A8m_v2	8	64	80	8000/160/80	16/16x500	8	2000

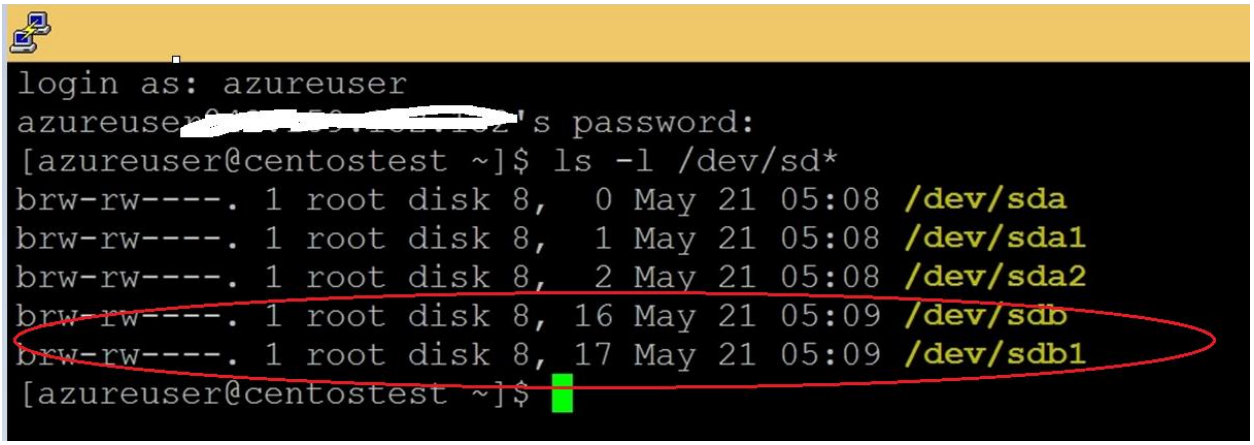
4.4.3 Azure 临时磁盘

1. 我们在 Windows 本地计算机就可以看到一块 D 盘:



- C 盘是操作系统盘，重启数据不会丢失。
- D 盘是临时磁盘，只能用来保存临时文件。临时盘数据会有丢失的风险。这块盘的 IOPS 会比较高，我们可以把临时文件保存在这块盘上。Azure 系统在有需要的时候会用它作为页面文件的临时存放点。
- E 盘是通过管理界面挂载上去的磁盘，重启数据不会丢失。

2. 在 Linux 操作系统里临时盘的名字是 sdb,如以下视图:



3. 有关更多临时盘的说明请参阅官方文档：
https://docs.azure.cn/zh-cn/articles/azure-operations-guide/virtual-machines/aog-virtual-machines-temporary-disk-instruction

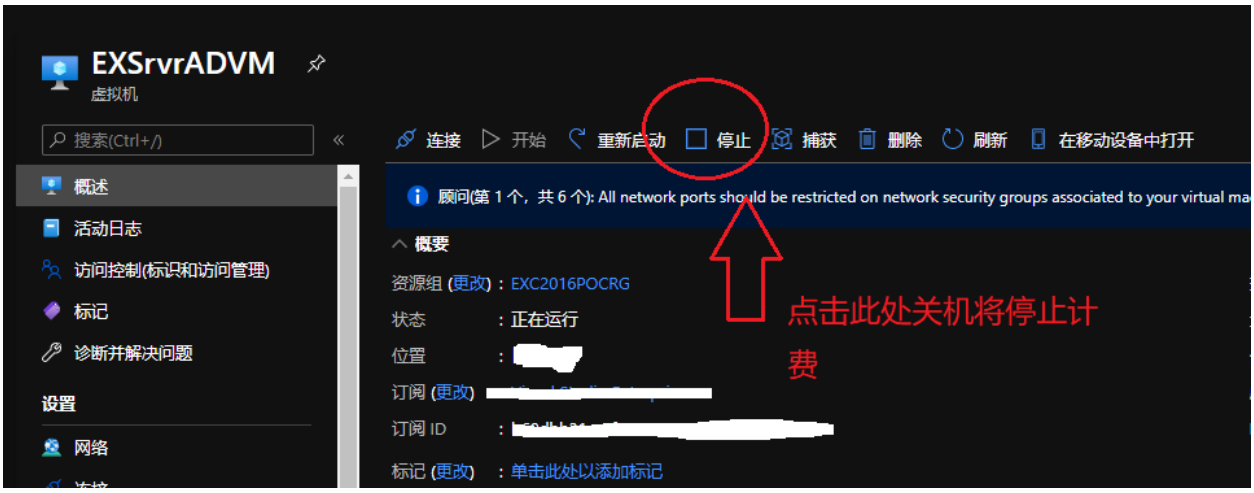
4.4.4 卸载磁盘

在某些情况下我们需要卸载虚拟机的磁盘，此时可以通过 Azure 管理界面选择这台虚拟机，然后点击分离磁盘：

4.4.5 虚拟机关机注意事项

如果我们通过远程桌面连接（RDP）或者是 SSH 关闭 Azure 虚拟机，是会继续收取 Azure **计算费**用的。

只有通过 Azure 管理界面关几才不会继续计费。但是因为虚拟机所在的 VHD 文件还没有被删除。所以虽然不会收取计算费用，但是虚拟机磁盘的**存储费**用还是会继续收取的：

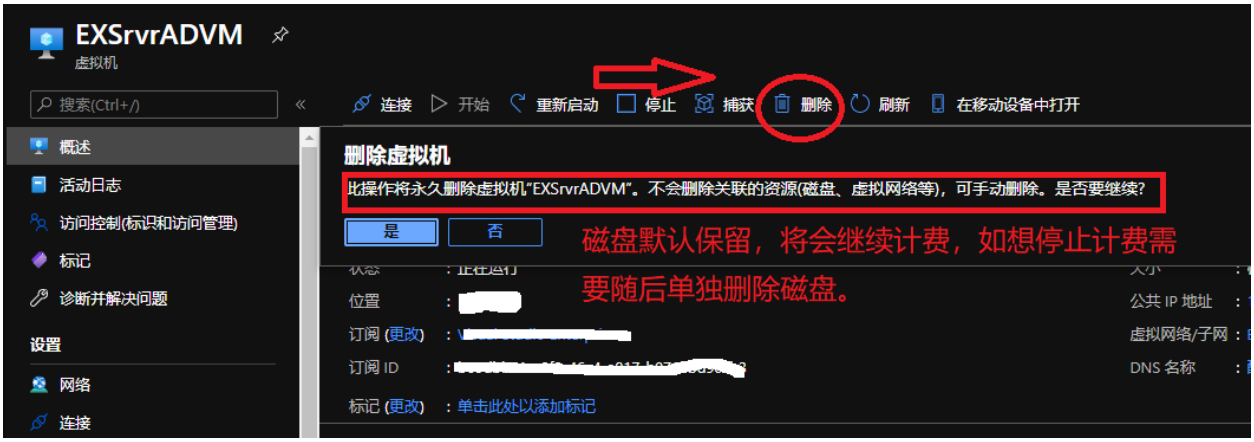


注：计算费+存储费=虚拟机实际计费。

4.4.6 删除 Azure 虚拟机

Azure 没有“回收站“功能。删除虚拟机之前必须确认该虚拟机里的文件已经做好备份。

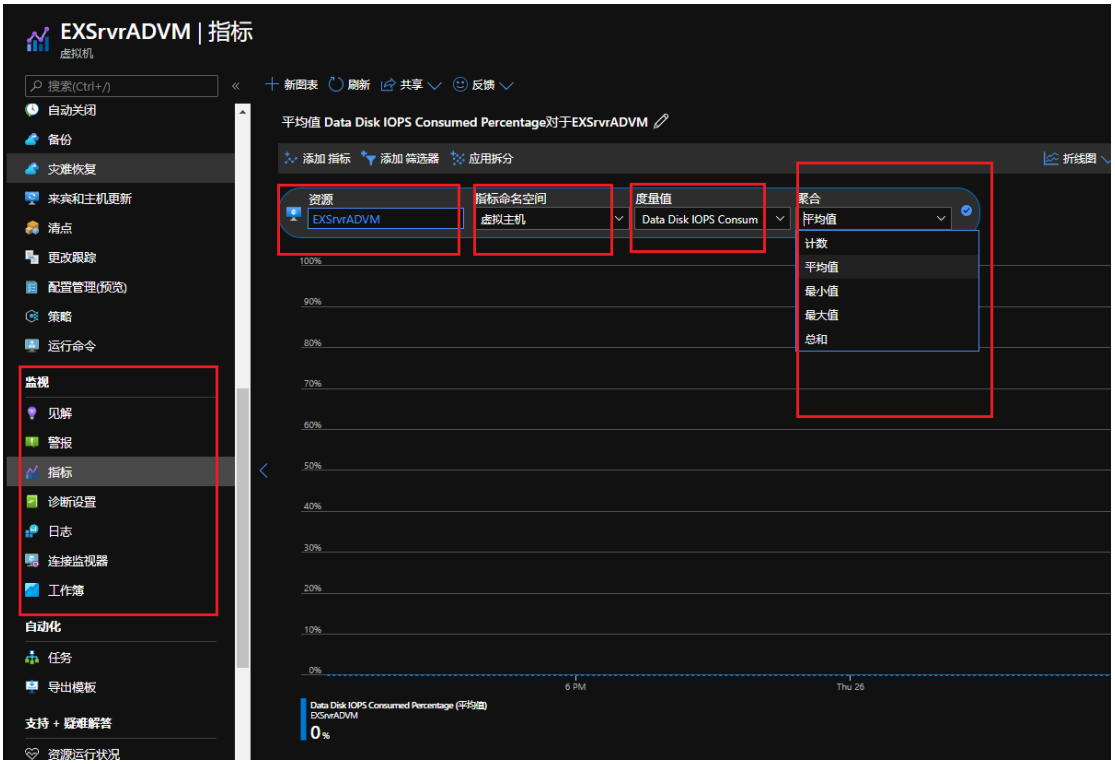
选中该台虚拟机然后点击删除，如下：



注：我们看到磁盘默认保留，这是为了数据安全防止误删除的设计。磁盘保留需要收取存储费用。如果想彻底停止计费需要随后删除其磁盘。

4.4.7 虚拟机监控

微软 Azure 虚拟机可以提供监控的功能，包括 CPU 使用率，磁盘读写，输入网络流量等。下图是快速入门举例：



以下是监控的专题:

https://docs.azure.cn/zh-cn/azure-monitor/overview

5. 运维部分

5.1 权限管理

假设 Contoso 公司购买了 Azure 合同，笔者建议：

1. Azure 企业管理员账户(拥有查看 Azure 账单的权限)。Contoso 公司的财务管理员维护。
2. Azure 账户管理员(拥有管理订阅的权限)。Contoso 公司的 IT 管理员维护。
3. 软件供应商(Software Vendor)。不需要提供 Azure 的账户，而是把虚拟机的远程桌面连接或者 SSH 提供给 Vendor，让 Vendor 通过远程桌面连接来部署相应的软件。Azure 虚拟机的端口需要在 IT 管理员的协助下进行配置。
4. 第三方技术支持(Partner & Visitor)。可分配 Guest 账号，并启用 MFA。然后通过 RBAC 仅针对相应需要支持 Azure 服务开放权限。

5. 基于角色的访问控制 (RBAC) 。设计 RBAC 授权时，请依照以下几点：
   - 用户分配角色时，要遵循最小特权原则
   - 细粒度的控制是很好的，但不要陷入不必要的复杂性。如果要创建仅适用于整个组织中的一个或两个人的角色，则可能有点过于复杂。有时简单意味着效率。
   - 同样，不要一开始就被角色分配所困惑。可以从几个关键角色开始，然后根据需要扩展。RBAC 内置角色很多，但这并不意味着您需要所有或大多数角色。
   - 在部署角色之前，可先对其进行测试。即可推出一个不完善的角色结构，这样充其量您可能会收到大量用户的权限请求；然而权限过大，可能会引发您的数据泄露。
   - 角色不一定是静态的，应定期检查您的角色分配，并根据需要进行调整。

5.2 Azure 治理

拥有正确的治理框架和流程以从 Microsoft Azure 中获得最大利益，并使环境更加健壮，安全，高效对于企业来说是至关重要的。企业 IT 需要确保数据和系统受到充分保护，同时又要与快速满足客户需求(内部和外部)保持平衡。

Azure 中的治理可结合以下 Control Mechanism 进行管控：

Tags：标签是与资源组本身关联的文本，您可以利用它对资源组进行分类

Locks：通过对资源组创建锁，可以防止意外删除或更改资源组中的资源

RBAC：提供访问不同资源的方式，让用户在资源组内仅执行某些操作的能力

Azure 策略：其是用于控制该资源组中某种行为或影响。比如，允许您创建，分配和管理策略以强制执行资源规则。

5.3 虚机部分

5.3.1 虚拟机关机

我们通过远程桌面连接或者是 SSH，关闭 Azure 虚拟机，是会继续收取 Azure 计算费用的。只有通过 Azure 管理界面(https://portal.azure.cn)，选中相应的 Azure 虚拟机，并点击关闭按钮。这样 Azure 虚拟机才不会继续收取计算费用

5.3.2 临时磁盘

Microsoft Azure 虚拟机磁盘中包含一个临时盘， D:磁盘 (Windows) 或者 /dev/sdb1 (Linux)。他们仅提供临时存储，所以可能会有丢失数据的风险且数据无法恢复。您可以将临时磁盘使用其他驱动编号，可参考官方文档。

5.3.3 虚拟机 DNS 修改

当我们在 Azure 中部署 AD DS 环境，或其他需要修改 Azure VM 的 DNS 指向时，一定要通过 Azure Portal 进行填写，禁止直接在 Azure VM 中直接修改，否则将无法 RDP 到此 VM，需以 image 重新部署才可恢复。

5.3.4 RDP 连接安全性

当我们创建完 Azure 虚拟机后，默认会打开远程桌面连接(Remote Desktop)和 SSH 连接，并且通过端口映射，将端口映射为高端口号。但是在互联网上还是有不怀好意的黑客会去扫描我们的虚拟机端口，并且频繁尝试访问，试图攻破虚拟机。

我建议：

1) 当使用完 Remote Desktop，请在 Azure 管理界面删除相应的 Public Port。阻止任何人通过 Public Port 访问远程桌面连接。
2) 使用 Azure 堡垒机进行连接
3) 使用 JIT VM 访问进行控制

5.3.5 Azure Update Management

Azure 更新管理解决方案是 Azure 自动化的一部分。借助 Azure 更新管理，您可以在 Azure，本地环境或其他云提供商中管理 Windows 和 Linux 计算机的操作系统更新。亦可以与现有的更新源（例如 Microsoft Update，WSUS）一起使用，以及将其集成到 System Center Configuration Manager 中。详情请参考此处

5.3.6 监控基础架构

建议使用 Azure Monitor 来查看资源的运行状况。Azure Monitor 功能：

资源诊断日志文件：监视您的 VM 资源并识别可能影响性能和可用性的潜在问题。

Azure Diagnostics 扩展：在 Windows VM 上提供监视和诊断功能。您可以通过将该扩展作为 Azure Resource Manager 模板的一部分来启用这些功能 。

不监视虚拟机性能的组织无法确定性能模式的某些更改是正常还是异常。虚拟机消耗的资源比正常多，可能表示来自外部资源的攻击或虚拟机中运行的进程受到威胁。

5.4 网络部分

5.4.1 Azure 虚机带宽

Azure 提供了与其他云厂商完全不同的带宽分配模式。Azure 的虚机规格型号越高，出站带宽就越高，配置多个网络接口无法增加虚拟机的总出站带宽，入站流量不计费；另外 Azure 内网流出也是会占用带宽，所以在不同规格的 VM 之间的网络吞吐量将取决于小规格的 VM；当然 VM 挂载的磁盘亦是如此。详细请参考官方链接.

5.4.2 压力测试

Azure 本身提供 Anti-DDos 功能。当我们在项目上线之前，会通过客户端压力测试工具对 Azure 服务进行压力测试。这时候就需要预先填写 Azure 渗透性测试表：https://docs.azure.cn/zh-cn/security/fundamentals/pen-testing

根据测试表中的内容，告知世纪互联测试时间、测试方法和测试客户端 IP 地址，这样世纪互联会提前把客户端 IP 地址加入到微软 Azure IP 白名单里，保证压力测试正常进行。

如果不提交渗透性测试表，会出现由于某个 IP 地址过于频繁访问 Azure 服务而被 Anti-DDos 设备禁用，造成压力测试失败。

5.5 存储部分

5.6 托管磁盘和非托管磁盘

其区别在于托管磁盘由微软后台为您提供不限 IOPS 和容量大小的磁盘，我们不用管理他们，当然如果您创建 1T 那么不管您实际使用了 10G 还是 100G，都是按照 1T 来收费；非托管磁盘是需要用户自己管理，用户需要考虑每一个存储帐号下的最高 IOPS 是 2 万，最大大小是 8T，当然用户是可以创建多个存储帐户的；非托管磁盘就是创建了 1T 的磁盘，也会按照实际使用多少算钱，比如用了 10G 就收 10G 的钱。

5.6.1 Azure Storage Explorer

使用 Azure 存储资源管理器可以更方便地对 Azure Storage 进行管理

5.6.2 Azure Storage 数据迁移

工作中时常会有将数据迁移到 Azure，或本地重用的场景。那么遇到这种情况您可有多种方式进行选择，每种方式使用的场景是不大相同的，总结起来可分为以下：

网络传输：

图形化界面(Azure Storage Explore 或 Azure 门户中基于 Web 的浏览工具)

AzCopy:https://docs.azure.cn/zh-cn/storage/common/storage-ref-azcopy?toc=/storage/blobs/toc.json

PowerShell:https://docs.azure.cn/zh-cn/storage/blobs/storage-quickstart-blobs-powershell

CLI :https://docs.azure.cn/zh-cn/storage/blobs/storage-quickstart-blobs-cli

SDK :https://docs.azure.cn/zh-cn/storage/blobs/storage-quickstart-blobs-java

Azure Data Factory: https://docs.azure.cn/zh-cn/data-factory/copy-activity-overview

物理传输：

Azure Import/Export : https://docs.azure.cn/zh-cn/storage/common/storage-import-export-service?toc=/storage/blobs/toc.json

Azure Data Box Disk: https://docs.azure.cn/zh-cn/databox/data-box-disk-quickstart-portal

我们可以选择的方式不少，但是具体哪种合适，还是要 case by case 来看；

首先，网络传输一个最大的弊端就是速度较慢，稳定性差，如果我们有大规模的数据需要传输到云上的话（比如 10T+），建议最好不要使用网络传输，速度不可控，对带宽依赖性非常强，并且还有传输中断的风险，对于这种大规模数据，更推荐使用 Azure import/Export 这种物理方式进行传输，直接把数据拷贝到硬盘里，加密之后直接寄送到数据中心，速度绝对是要快得多的

其次，如果数据量比较少的话，那么网络传输比物理传输优势会更明显，在这么多种网络传输的方案里，更推荐使用 azcopy，azcopy 出来的时间已经很久了，现在最新版是 azcopy v10，v10 的使用比以前要更简单，还能支持使用 Azure AD 进行身份验证

如果您想要利用 AzCopy 的性能优势，但同时又偏好使用图形用户界面而不是命令行来与文件进行交互，则可以使用 Azure 存储资源管理器。

AZCopy: azcopy | Azure Docs

5.7 备份和灾备

Azure 上的备份方案主要有两个：Azure 备份（Azure Buckup）和 Azure Site Recovery，两项服务都提供不同但互补的功能，但两者有一些典型的区别：

Azure Site Recovery：Site Recovery 为本地计算机和 Azure VM 提供灾难恢复解决方案。可以将计算机从主位置复制到辅助位置。 出现灾难时，可以将计算机故障转移到辅助位置，从辅助位置访问它们。一切恢复正常后，可以对计算机执行故障恢复，在主站点恢复它们。

Azure 备份：Azure 备份服务可以从本地计算机和 Azure VM 备份数据。可以在粒度级别备份和恢复数据，包括对文件、文件夹和计算机系统状态进行备份，以及进行应用感知型数据备份。Azure 备份处理数据时所在的粒度级别比 Site Recovery 更细。比如，如果便携式计算机上的演示文稿损坏，则可使用 Azure 备份来还原该演示文稿。若要确保 VM 配置和数据的安全性和可访问性，则可使用 Site Recovery。

Azure Backup 支持备份本地计算机和 Azure VM，备份相关的几个概念和术语：

- MABS(Microsoft Azure Backup Server)：更多 MABS 的信息，请参考官网：https://docs.azure.cn/zh-cn/backup/backup-azure-microsoft-azure-backup
- MARS(Azure Recovery Services agent):一个代理程序，可以从 Azure Backup 控制台下载。更多 MARS 的信息，请参考官网：https://docs.azure.cn/zh-cn/backup/backup-azure-about-mars
- DPM(Data Protection Manager):DPM 备份文件和应用数据，DPM 是部署在物理机上或者本地虚机上，DPM 可以备份数据到 Azure Backup Valult 上。更多 DPM 的信息，请参考官网：https://docs.azure.cn/zh-cn/backup/backup-azure-dpm-introduction
- 备份服务器(Backup Server)：通常是指本地的 System Center Data Protection Manager (DPM) 或者 Azure 备份服务器（ Azure Backup Server (MABS)）

备份本地计算机

1) 在本地 Windows 计算机上运行 Azure 备份服务的 Azure 恢复服务 (MARS) 代理，以备份单个文件和系统状态。
2) 将本地计算机备份到备份服务器（System Center Data Protection Manager (DPM) 或 Azure 备份服务器 (MABS)），然后将备份服务器配置为备份到 Azure 中的 Azure 备份恢复服务保管库。

备份 Azure VM

1) 为单个 Azure VM 启用备份。启用备份时，Azure 备份会在 VM 上运行的 Azure VM 代理中安装一个扩展。该代理备份整个 VM。
2) 在 Azure VM 上运行 MARS 代理。 若要备份 VM 上的单个文件和文件夹，此功能将十分有用。

3) 将 Azure VM 备份到 Azure 中运行的 DPM 服务器或 MABS。然后使用 Azure 备份将 DPM 服务器/MABS 备份到保管库。

SQL Server 备份

如果需要备份 SQL Server 工作负荷，可使用其他选项。Azure 备份可以在 Windows 上的 SQL Server 实例上安装工作负荷备份扩展，以支持以下选项：

- **完整**：备份整个数据库和文件组。它还包含足够的日志来执行还原。事务日志会保存数据库中记录的最新添加或删除记录。要执行数据库的最新还原，需使用最新的事务日志。
- **差异**：基于上次执行的完整备份，仅捕获自上次完整备份后更改的数据块。
- **事务日志**：允许进行数据库的时间点还原。
- Linux 上的 SQL Server 当前未与 Azure 备份集成

案列：

从 Azure Backup 备份 Azure VM

备份 Azure VM 中 SQL Server 数据库

将文件从 Azure 恢复到 Windows Server

5.8 安全配置

Azure 中有以下三个服务可进行安全配置及其管理：

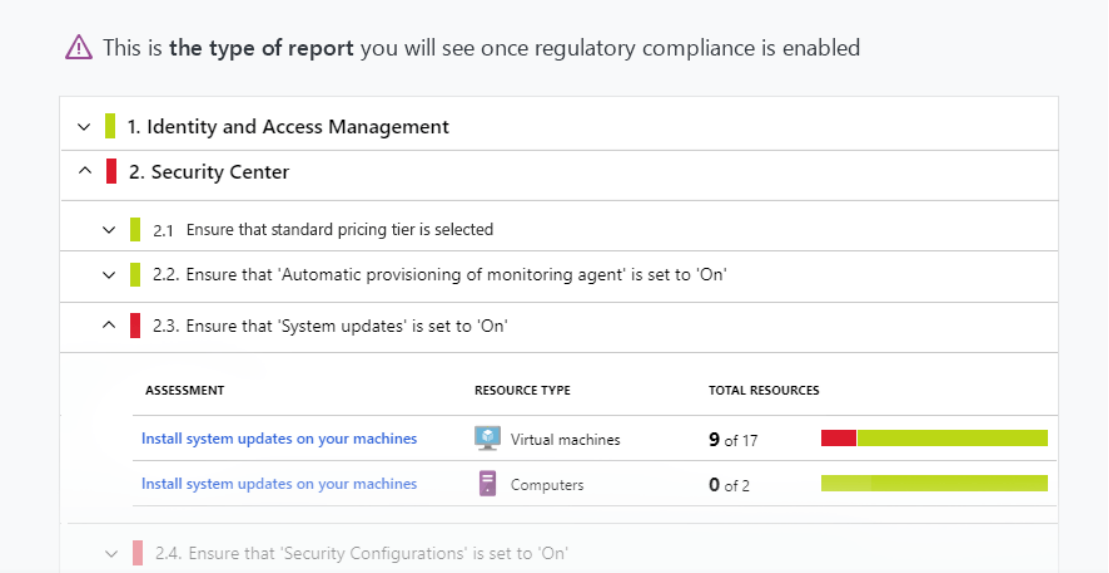
安全组 Network Security Group（简称 NSG）用来筛选 Azure 虚拟网络（virtual network）中出入 Azure 资源的网络流量。NSG 包含安全规则，安全规则是允许或拒绝入站/出站流量的规约。但其受限与 Azure 订阅限制：每个订阅最多 5000 网络安全组，每个 NSG 最多 1000 条 NSG 规则。

Web 应用程序防火墙（Web Application Firewall，通常简称 WAF）是通过执行一系列针对 HTTP/HTTPS 的安全策略来专门为 Web 应用提供保护的一款产品。

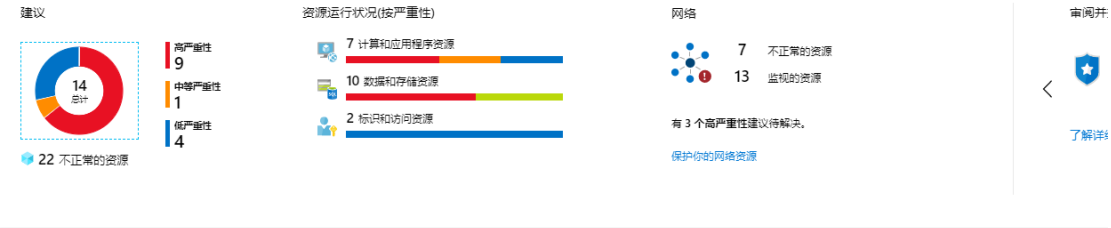
Azure 安全中心是一个统一的基础结构安全管理系统，可以增强数据中心的安全态势，以及为云中（无论是否在 Azure 中）和本地的混合工作负荷提供高级威胁防护。

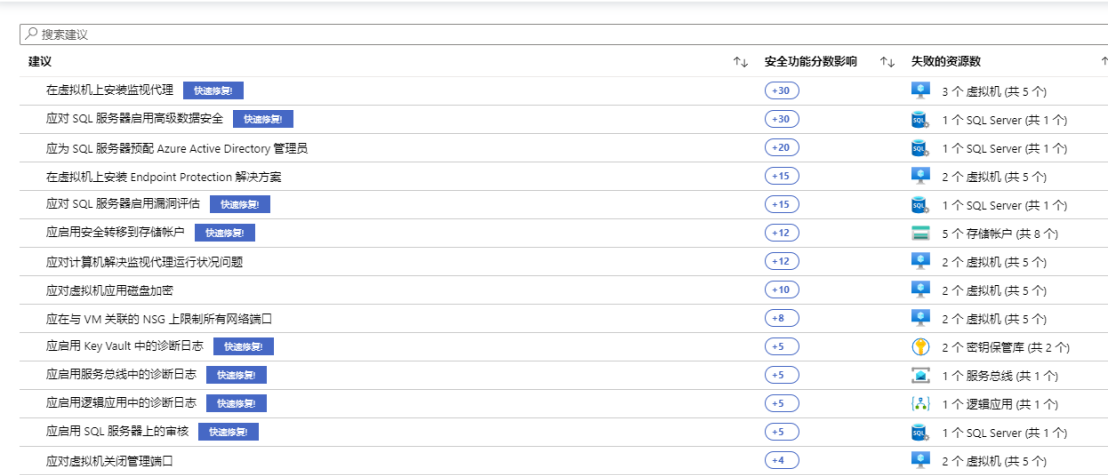
安全中心可在如下方面帮到我们：

法规符合性，是否满足 ISO27001 等法规的要求，并给出处理建议

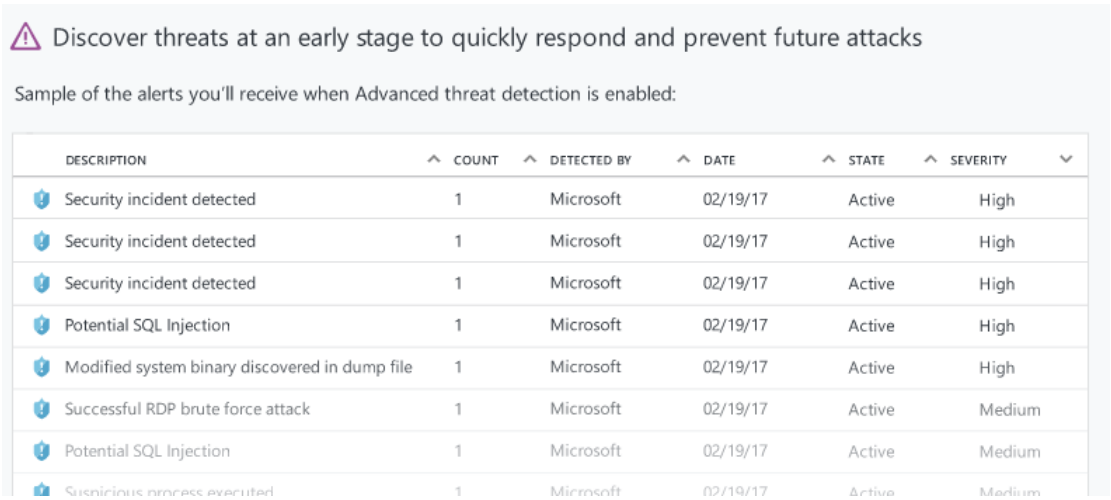


各资源（虚拟机/网络/数据库/存储等等）的配置是否安全，并给出处理建议



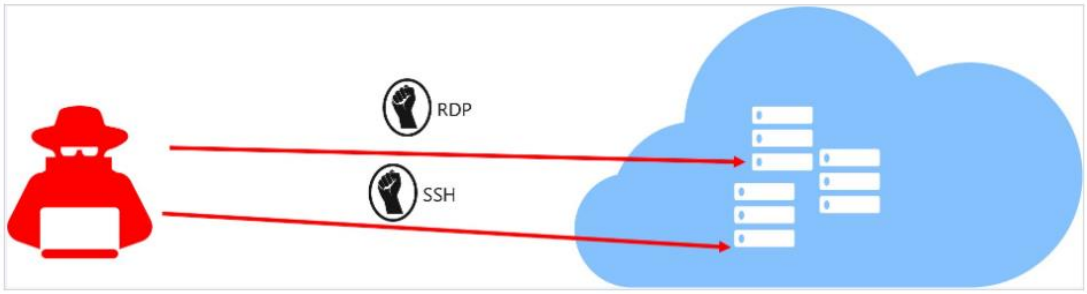


提供高级威胁检测及报警



其他 高级云防御，比如 实时 VM 访问（Just-in-time (JIT) virtual machine (VM) access）

降低遭受暴力攻击的可能性的一种方法是限制端口处于打开状态的时间量。 管理端口不需要始终打开。 只需在连接到 VM 时打开这些设备，例如执行管理或维护任务。 启用实时时，安全中心会使用网络安全组（NSG）和 Azure 防火墙规则，这些规则将限制对管理端口的访问，从而使攻击者无法针对这些端口。



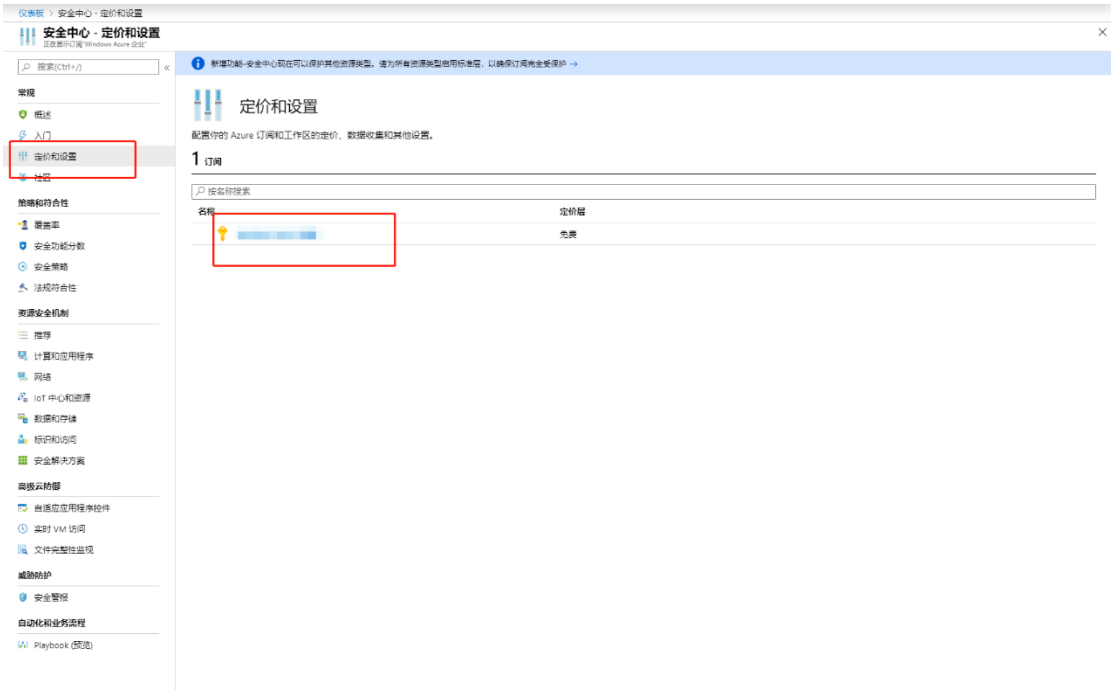
如果启用了实时访问，安全中心会通过创建 NSG 规则来锁定发往 Azure VM 的入站流量。 你需要选择要锁定 VM 上的哪些端口的入站流量。 这些端口将受实时解决方案控制。

当用户请求访问 VM 时，安全中心会检查该用户是否具有该 VM 的基于角色的访问控制（RBAC）权限。 如果批准了请求，安全中心会自动将网络安全组（NSG）和 Azure 防火墙配置为允许所选端口的入站流量，并在指定的时间范围内请求源 IP 地址或范围。 在该时间到期后，安全中心会将 NSG 还原为以前的状态。 但是，那些已经建立的连接不会中断。

安全中心层级

Azure 安全中心跨混合云工作负荷提供统一的安全管理和威胁防护。**免费层只能为 Azure 资源提供有限的安全性，而标准层将这些功能扩展到了本地和其他云**。借助安全中心标准层，可以查找和修复安全漏洞、应用访问控制和应用程序控制来阻止恶意活动、使用分析和智能功能检测威胁，以及在受到攻击时迅速做出响应。可以免费试用安全中心标准版。

升级到标准层：

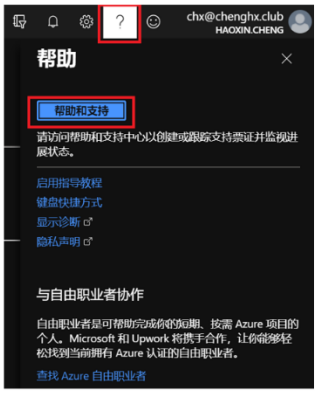

仪表板 > 安全中心 - 定价和设置
安全中心 - 定价和设置
搜索(Ctrl+/)
常规
概述
入门
定价和设置
策略和符合性
覆盖率
安全功能分数
安全策略
法规符合性
资源安全机制
推荐
计算和应用程序
网络
IoT 中心和资源
数据和存储
标识和访问
安全解决方案
高级云防御
自适应应用程序控件
实时 VM 访问
文件完整性监视
威胁防护
安全警报
自动化和业务流程
Playbook (预览)
定价和设置
配置你的 Azure 订阅和工作区的定价、数据收集和其他设置。
1 订阅
按名称搜索
名称
定价层
免费


仪表板 > 安全中心 - 定价和设置 > 设置 - 定价层
设置 - 定价层
搜索(Ctrl+/)
设置
定价层
数据收集
电子邮件通知
保存
标准层提供增强的安全性。了解更多 >
免费(仅适用于 Azure 资源)
标准
持续评估和安全建议
Azure 安全功能分数
实时 VM 访问
自适应应用程序控制和网络强化
合规性仪表板和报表
用于 Azure VM 和非 Azure 服务器(包括服务器 EDR)的威胁防护
用于受支持 PaaS 服务的威胁防护
定价适用于此订阅中的 6 个资源
按资源类型选择定价层
资源类型
资源数量
定价
计划
虚拟机
5 个 VM 和 VMSS 实例
144 人民币/服务器/月
已启用
已禁用
PaaS SQL Server
1 个资源
144 人民币/服务器/月
已启用
已禁用
单击"保存"会为选定资源类型启用标准层。前 30 天免费。
若要详细了解安全中心定价，请访问定价页。

5.9 开启支持工单

如何开工单?

第一个入口 -通过全局标头转到“帮助 + 支持



第二个入口 -通过资源菜单转到“新建支持请求”
每个Azure资源的最下面都有创建工单的链接

5.10 ICP 备案

1. 默认情况下，创建的 Azure 服务默认使用的 DNS 地址为:Chinacloudapp.cn、Chinacloudapi.cn 和 Chinacloudsites.cn，域名由上海蓝云网络科技有限公司备案，仅用于向其客户提供 Azure 服务。如果您需要通过 Azure 平台对外提供服务，应使用自有的域名提供服务，并根据相关规定对自有域名做相应的 ICP 备案。通过 Internet 访问应用服务，仅可通过已完成 ICP 备案的自定义域名进行访问，任何通过应用服务默认域名的访问将会被封堵。
2. 客户自有域名 ICP 备案可以通过各种域名备案组织和世纪互联代理；但如果指向国内 Azure 的 IP 地址和 Azure 服务，需要用户到世纪互联提交备案，具体详细备案信息以及流程请参考此处；如果客户的根域名(contoso.com.cn)在没有备案的情况下，做了 A 记录解析到 Azure 的公网 IP 上，(如 http://azure.contoso.com.cn 的 A 记录，指向到微软 Azure 的公网 IP 43.192.xxx.xxx)
   工信部在进行审查的时候，如果根域名没有进行备案，会要求世纪互联尽快关闭该网站。
   世纪互联目前的流程是，先通知用户在规定时间内按要求对网站进行关闭。如用户不能在规定时间内按要求完成，或世纪互联无法联系到用户时，会采取暂停用户部署或订阅服务。
3. 如果客户之前在 IDC 托管机房，或者其他网络接入商(如万网等)注册过顶级域名(contoso.com.cn)，且该域名指向的公网 IP 地址不在微软 Azure 云平台。现在需要将 IP 指向到微软 Azure 云平台，根据现有的备案要求，需要用户到世纪互联提交备案信息，做新增接入操作。具体请联系世纪互联，具体详细备案信息以及流程请参考此处。
4. ICP 备案周期：在您提交信息后，世纪互联会在 2 个工作日进行初审；若审核通过，世纪互联会通知您来公司进行现场核验；面签通过后，世纪互联会在收到纸质资料和照片后 1.5 个工作日进行二次审核，并将信息提交到省管局，管局会在 20 个工作日内下发审核意见。

5. 如果客户使用的域名为新注册或未在其他 IDC、网络接入商使用，需要在世纪互联进行 ICP 备案后的一个月内进行公安备案(自行完成)。具体详细备案信息以及流程请参考此处。
6. 其他热点问题请参考 F&Q。

5.11 Azure 和 O365 同时使用

对于 Microsoft Azure 订阅，最高级别的管理为租户。默认情况下，当您创建第一个 Azure 订阅时，就会创建一个租户。

如果您已经在使用 Office365，其实您已经拥有一个 Azure AD 租户。Office 365 和 Azure 同时使用 Azure Active Directory 来管理活动目录。我们遇到过许多客户在已使用 Office 365 的情况下，再创建新 Azure 租户的错误。问题在于，原 Office 365 租户已有绑定的 Azure Active Directory，而再次创建新的 Azure 租户会创建 Azure Active Directory 的新目录。这使 Azure Active Directory 难以管理，员工也将需要使用多个账号来访问公司资源。那么您可以通过 Office 365 账号直接购买 Azure 订阅，可参考此处链接或联系 Microsoft 购买 Azure 企业合约。

6. Azure 学习资源

云计算服务 | Microsoft Azure: Azure Global 官网

Azure 云计算–安全可信的智能云服务平台: Azure China 官网

Microsoft Azure Learn: 系统化的 Learning Path，认证

Microsoft Cloud Workshop: 场景模拟，动手实践

Azure China 常用操作指南