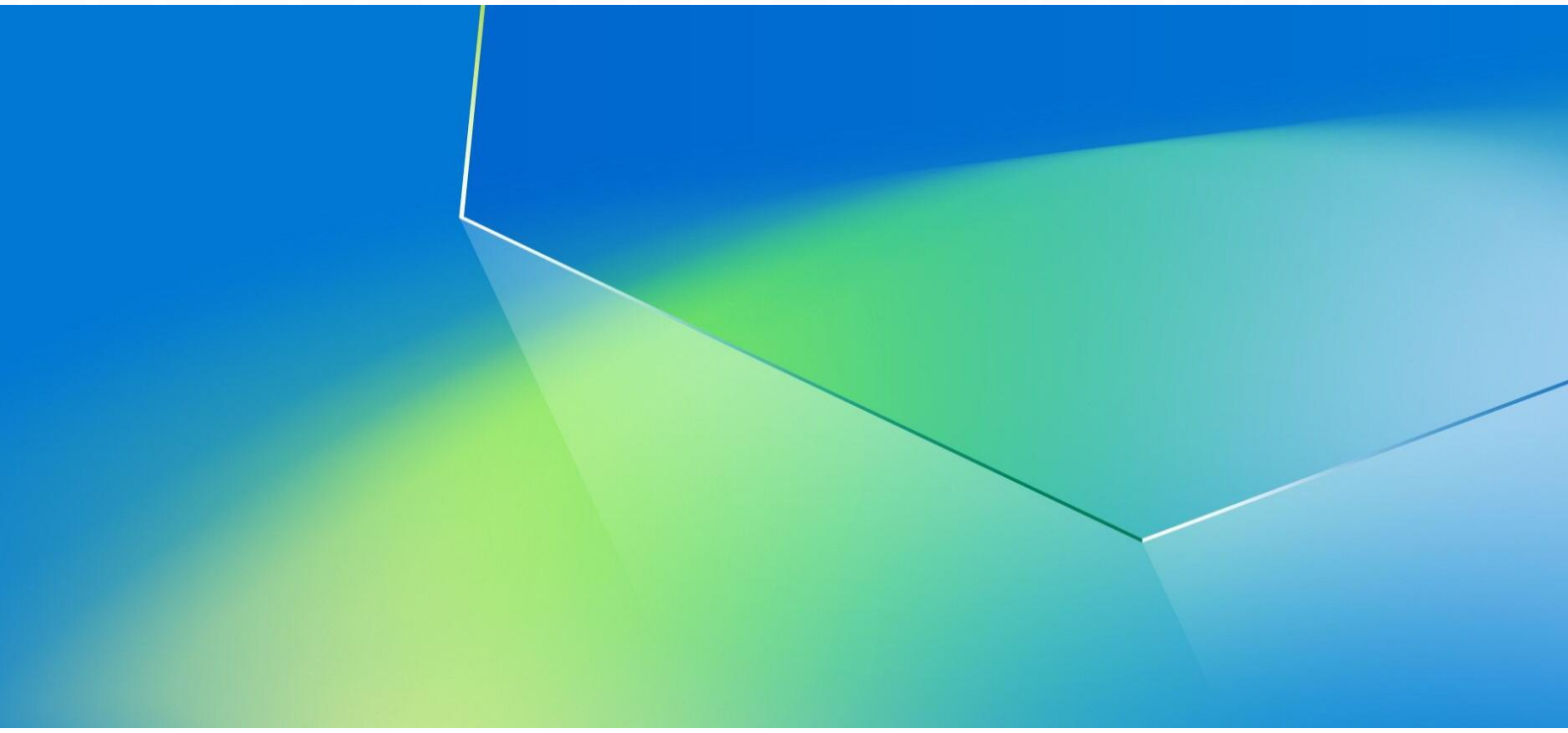
Microsoft Azure 由 世纪互联 运营

Azure 中国云

用户迁移指南

V1.1



发布日期 2025.6

目 录

版本历史 3
Azure 中国云用户迁移指南 4
区域选择使用指南 5
迁移过程 7
Azure 资源跨区域迁移手册 11
迁移 Azure Firewall 14
迁移 Azure Key Vault 20
迁移 Azure Managed Disks 25
迁移 Azure Storage Account 28
迁移 Azure 流分析作业 32
迁移 Azure Synapse Analytics 工作区 36
HDInsight 50
迁移 Azure 自动化 52
迁移 Azure Monitor 53
迁移 Azure Site Recovery 56
迁移 Azure Backup 57
迁移 Azure Event Hubs 59
迁移 Azure Event Grid 61
迁移事件网格域 63
迁移事件网格系统主题 68
迁移事件网格自定义主题 73
迁移 Azure Logic Apps 77
迁移 Azure Service Bus 79
迁移 Azure Functions 81
迁移 Azure Virtual Desktop 83
迁移 Azure Batch 服务 85
迁移 Azure Cloud Services 90
迁移 Azure Virtual Machine 94
迁移 Azure Virtual Machine Scale Sets (VMSS) 98

迁移 Azure Application Gateway 100
迁移 Azure Bastion 资源 102
迁移 Azure DNS 104
迁移 Azure ExpressRoute 实例 106
迁移 Azure Public IP 107
迁移 Azure 路由服务器实例 108
迁移 Azure Traffic Manager 110
迁移 Web Application Firewall (WAF) 114
迁移 Azure Load Balancer 115
迁移 Azure NAT 网关 126
迁移 Azure Network Watcher 127
迁移 Azure 专有链接服务实例 128
迁移 Azure Virtual Network 130
迁移虚拟 WAN 136
迁移 Azure VPN 网关 143
迁移 Azure Container Registry 145
迁移 Azure Service Fabric 148
迁移 Azure Analysis Services 152
迁移 Azure Cache for Redis 153
迁移 Azure Database for MySQL 158
迁移 Azure Database For PostgreSQL 160
迁移 Azure SQL 资源 161
迁移 SQL Server Stretch Database 163
迁移 Azure API 管理 164
迁移 Azure 应用服务 166
迁移 Azure IoT Hub 175
迁移 Notification Hubs 180

版本历史

日期	版本	变更说明
2025/05/21	1.0	初始发布
2020/06/04	1.1	添加了资源组（Resource Group）和操作组（Action Group）的迁移说明

Azure 中国云用户迁移指南

由世纪互联运营的 Microsoft Azure (简称 Azure 中国云)是在中国大陆独立运营的公有云平台，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，目前在东部和北部分别各部署有数据中心。

理论上讲，云计算资源在一定条件下可以近似认为是无限的。但是由于云计算技术的快速发展，及中国互联网业务的高速成长，要求云服务的基础设施的建设速度及建设方式需要不断根据需求进行动态调整，以满足不断增长及变化的业务需求。对于由此而带来的潜在风险，需要用户充分了解云服务的特性，并对基于云服务搭建的系统进行适配及调整，以提高系统的灵活性及稳定性。

本指南用于指导 Azure 中国云用户安全、高效地将北部 1 区和东部 1 区现有 Azure 资源迁移至中国其他区域。包含以下内容：

- 区域选择指南
- 迁移过程详解
- 资源迁移手册

区域选择使用指南

区域特性差异

由于中国云的客户在地域分布，所属行业，产品/服务/IT 系统周期等不同维度的需求上有很大差异，所以中国云各区域在根据客户需求的不断调整迭代中，也会演进出相应的各区域的独特特性以适应中国云各区域客户的业务发展需求。

了解这些差异，并在系统落地、扩容、升级及重构过程中更好地利用这些差异，能够帮助系统架构从设计上实现长期适配所部署区域，降低由于各种外部因素变化对客户造成的潜在影响。

区域服务差异

Azure 中国云各区域根据其客户特性及需求，其在各区域的具体服务部署进度也会有所差异，具体差异可参照 Azure 中国可用服务，这个列表会定期更新，保证用户获得最新的信息。另外，访问 Azure 更新页面可以获得 Azure 新服务上线的全部公告。

行业分布差异

由于某些行业客户的业务或用户会集中在某些热点地区或时间段，因此会造成在这些地区或时段对资源的需求集中释放，从而造成资源紧张。

- **零售行业**：零售行业是中国云业务的重点行业之一，尤其是近几年中国消费市场的飞速成长及新零售相关业务的蓬勃发展，因此无论是本土企业还是海外企业都把中国当成了全球重要的消费市场进行开发，尤其是中国东部的长三角地区以及南部的珠三角地区，是零售企业的重点业务拓展区域。所以，各公有云服务企业在中国东南部地区部署的云资源中，零售行业客户都是重要的资源消耗者。特别是在零售行业的热点活动季节，比如“双十一”，更是各企业对云服务需求的集中释放时间，导致这些时间段的资源紧缺。

- **高级资源分布差异**：对于 SSD 硬盘，GPU 服务器等高级资源，由于前期投入比较高，所以其资源投入的速度是建立在各区域的潜在业务需求分析，然后根据增长趋势的预测分阶段按需投入的。因此相比于普通资源，高级资源价格相对会高，资源数量也会受限。然而合理使用高级资源能够有效降低运营成本，同时提高系统的健壮性。

    - 高级托管磁盘：高级托管磁盘是基于高性能 SSD 存储资源硬件设施的，如果在某些区域被大量集中使用，会造成一段时间的资源相对紧缺，从而对该区域客户的业务发展产生影响。
    - GPU 资源：GPU 资源目前已经在北部 2 区、北部 3 区和东部 2 区上线，如果用户有对 GPU 资源的需求，推荐使用北部 3 区（支持的 GPU 型号参考：NC 系列和 NV 系列 SKU 列表，需要在北 3 区域申请对应 GPU 机型的配额）。

- 多 AZ 部署：中国北 3 区域带来了 Availability Zone 高可用能力，可为企业关键业务应用提供 99.99%的高可用保障，并提供更完善的灾备和恢复能力。

优化所用区域资源

您可以根据以下所介绍的规则对您的部署进行相应调整，以降低或消除隐患。

合理利用热点区域

对于客户并非集中在东部地区的 Azure 中国云用户，并且对时延要求不高的业务应用场景，应尽量使用北部 3 区的资源，以降低由于热点行业的热点活动造成的资源紧缺对您业务的潜在影响。

合理使用热点资源

对于高级资源，要根据您业务的具体业务指标合理使用。除非普通资源不能满足业务要求，否则尽量避免在不必要的场景使用高级资源，既提高了系统的健壮性，也降低了系统运营成本。

例如：

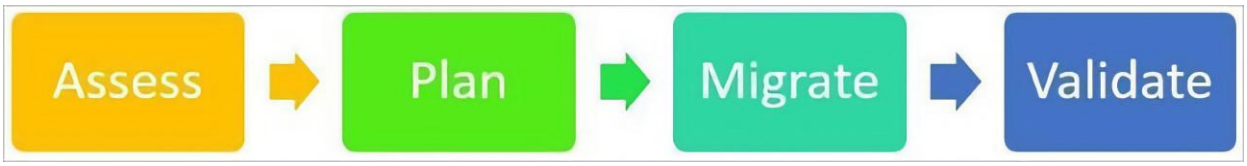
- 如果普通 HDD 能满足指标要求，在创建虚机资源时，**OS 磁盘类型** 选择**标准 HDD** 磁盘以替代默认选项 **高级 SSD** ，以减少对高级托管磁盘的依赖。
- 在创建快照时，**账号类型** 选择 **标准 HDD** 代替 **高级 SSD**。

有关更多信息：

- 查阅托管磁盘价格详情了解更多关于标准 HDD 及高级 SSD 的指标及价格差异。

迁移过程

本章节提供的指南可帮助您了解 Azure 资源从一个 Azure 区域迁移到另一个区域的整体过程。迁移过程的重点是如何制订出应用程序的整体迁移计划，然后依据迁移计划依次迁移 Azure 资源。 迁移过程中的步骤如下：



迁移过程

详细内容请参阅云采用框架 - 重新定位云工作负载。

评估

您应当召集 Azure 帐户所有者、订阅管理员、租户管理员以及金融和会计团队，以了解计划迁移的组织规模，这一点非常重要。担任这些职能的工作人员可提供大型组织对 Azure 使用的完整信息。 在评估阶段，编制一份资源清单：

- 每个订阅管理员和租户管理员应运行一系列脚本来列出资源组、每个资源组中的资源以及环境中的资源组部署设置。
- 您应当记录 Azure 中各应用程序之间以及与外部系统的依赖关系。
- 您还应当记录与要迁移的每个实例关联的每个 Azure 资源的数量以及数据量。
- 确保应用程序体系结构文档与 Azure 资源列表保持一致。

在此阶段结束时，您将拥有：

- 需要迁移的 Azure 资源的完整列表。
- 资源之间的依赖关系列表。
- 有关迁移工作复杂性的信息。

计划

在计划阶段，您应当完成以下任务：

- 使用在评估阶段完成的依赖关系分析的输出结果来定义相关组件。请考虑通过迁移包迁移相关组件。
- 确定目标 Azure 区域中的目标环境。
- 识别目标 Azure 租户，如果对迁移目标环境有新的管理需求（隔离、安全性等），可以创建一个新的 Azure 租户。
- 识别目标订阅，如果对迁移目标环境有新的管理需求（资源管理、成本管理等），可以创建一个新的订阅。

- 选择目标 Azure 区域。
- 执行使源 Azure 区域中的体系结构与目标区域中的体系结构相匹配的测试迁移方案。
- 确定合适的迁移时间线和计划表。为每个迁移包创建用户验收测试计划。

迁移

在迁移阶段，使用以下各节中讨论的工具、技术和建议在目标区域中迁移或创建新资源，然后配置应用程序。

验证

在验证阶段，完成以下任务：

- 完成用户验收测试。
- 如果适用，将最新数据同步到目标环境。
- 确保应用程序按预期工作。
- 切换到目标区域中的新应用程序实例。
- 验证生产环境是否按预期工作。
- 取消配置源区域中的资源。

术语

以下各节使用了这些术语：

源描述了从哪里迁移资源

- **源租户名称**：源 Azure 区域中租户的名称（帐户名称中 @ 之后的所有内容）。
- **源租户 ID**：源 Azure 区域中租户的 ID。将鼠标移到右上角的帐户名称时，租户 ID 将显示在 Azure 门户中。
- **源订阅 ID**：源 Azure 区域中资源订阅的 ID。您可以在同一个租户中拥有多个订阅。请始终确保您使用的是正确的订阅。
- **源区域**：迁出资源所在的区域。

目标或目的地是指接收迁移资源的目的位置

- **目标租户名称**：目标 Azure 区域中租户的名称。
- **目标租户 ID**：目标区域中租户的 ID。
- **目标订阅 ID**：目标区域中资源的订阅 ID。
- **目标区域**：接收迁移资源的目的区域。

注意

- 验证您要迁移的 Azure 服务是否在目标区域中提供。
- 北部 3 区支持多可用性区域服务，具体支持的服务清单请参阅：可用性区域服务和区域支持。
- 迁移前请确保进行了充分的测试和备份，以防止数据丢失。

Azure 资源跨区域迁移

迁移"全局"Azure 资源

某些 Azure 资源是全局服务（例如 Azure DNS 区域），根据定义，这些资源没有特定的位置。这些 Azure 资源无法设置为区域性位置。

如果目的是在同一云环境中将全局资源从一个区域迁移到另一个区域，通常只需将其移动到新区域中的资源组即可，无需执行其他操作。全局资源的位置本身无需更改。

这里的"全局"一词本质上意味着数据不绑定到某个具体区域，而是绑定到云本身。也就是说，即使资源的位置显示为"全局"，其数据也始终托管在该云的边界之内。

换句话说，托管在 Azure 中国云中的全局资源，其位置可能显示为"全局"，但它永远不会托管在 Azure 中国云之外。同样，托管在公共云中的全局资源也不会托管在 Azure 中国云中。然而，这些数据不会绑定到云中的某个特定区域，而是可以分布在同一云中的多个区域。

迁移"区域性"Azure 资源

有关如何跨区域迁移具体资源，请查阅 Azure 资源跨区域迁移手册章节的介绍。

跨区域迁移后的公网 IP 变更

当您将公网 IP 地址从一个区域迁移到另一个区域时，该公网 IP 地址将会发生变化。这是因为公网 IP 地址与其创建时所在的区域绑定。在迁移完成后，您需要更新所有引用旧公网 IP 地址的 DNS 记录或配置。

资源组迁移

在弃用区域下线之前，你应将资源组中的资源迁移到可用区域的资源组中，因为位于弃用区域的资源组将连同其元数据一并被删除。一旦元数据被删除，这些资源将无法执行创建、读取、更新和删除（CRUD）操作，因为系统将无法再引用这些资源。

如需了解如何在资源组之间移动资源，请参阅以下官方文档：

- 将 Azure 资源移到新的资源组或订阅

Azure 资源跨区域迁移手册

本章节中描述了各迁移阶段相关的迁移步骤。

资源评估

- 了解源环境和目的环境之间服务与配置的一致性
- 估算在目的环境中的运营成本
- 了解已部署资源之前的依赖关系
- 为决策和工作计划制定综合评估报告

迁移计划

- 根据资源之间的依赖关系，规划资源的迁移顺序
- 根据资源的迁移顺序，估算迁移所需时间
- 生成迁移计划报告

资源迁移方法

资源迁移必须依据用户最终确认的迁移计划，顺序依次迁移所部署的资源。

使用 Azure 资源移动器

使用资源转移器，当前可以在区域之间移动以下资源：

- Azure VM 和关联的磁盘（目前不支持 Azure 现成 VM）
- 已加密的 Azure VM 及关联磁盘。 这包括启用了 Azure 磁盘加密的 VM 和使用默认服务器端加密的 Azure VM（这两者都使用平台管理的密钥和客户管理的密钥）
- NIC
- 可用性集
- Azure 虚拟网络
- 公共 IP 地址（公共 IP 不会跨区域保留）
- 网络安全组 (NSG)：
- 内部和公共负载均衡器
- Azure SQL 数据库和弹性池

详细参考文档：Azure 资源移动器

通过手动方法迁移

- 迁移安全资源
  - Azure Firewall
  - Key Vault
- 迁移存储资源
  - Managed Disks
  - Storage Accounts
- 迁移分析服务
  - Azure Stream Analytics
  - Azure Synapse Analytics
  - HDInsight
- 迁移管理工具资源
  - Azure Automation
  - Azure Monitor
  - Azure Site Recovery
  - Azure Backup
- 迁移集成资源
  - Event Hubs
  - Event Grid
    - Event Grid Domain Migration
    - Event Grid System Topics Migration
    - Event Grid Custom Topics Migration
  - Logic Apps
  - Service Bus
- 迁移计算资源
  - Azure Functions
  - Azure Virtual Desktop
  - Batch
  - Cloud Services
  - Virtual Machines
  - Virtual Machine Scale Sets
- 迁移网络资源
  - Application Gateway
  - Azure Bastion
  - Azure DNS
  - Azure ExpressRoute
  - Azure Public IP
  - Azure Route Server
  - Azure Traffic Manager
  - Azure WAF
  - Load Balancer
  - NAT Gateway
  - Network Watcher

    - Private Link Service
    - Virtual Network
    - Virtual WAN
    - VPN Gateway
- 迁移容器资源
    - Azure Container Registry
    - Azure Service Fabric
- 迁移数据库资源
    - Azure Analysis Services
    - Azure Cache for Redis
    - Azure Database for MySQL
    - Azure Database for PostgreSQL
    - Azure SQL
    - SQL Server Stretch Database
- 迁移 Web 资源
    - API Management
    - App Service
- 迁移 IoT 资源
    - Azure IoT Hub
    - Notification Hubs

迁移 Azure Firewall

概述

Azure Firewall 是一种云原生的网络安全服务，提供高可用性和无缝的云缩放功能。本指南将帮助您将 Azure Firewall 从一个区域迁移到另一个区域。

先决条件

- 强烈建议使用高级 SKU。 如果你使用的是标准 SKU，请考虑在重定位之前使用 PowerShell 将 Azure 防火墙配置迁移到 Azure 防火墙策略。
- 为了正确规划和执行 Azure 防火墙重定位，必须收集以下信息：
    - **部署模型。**经典防火墙规则或防火墙策略。
    - **防火墙策略名称。** （如果使用防火墙策略部署模型）。
    - **防火墙实例级别的诊断设置。** （如果使用 Log Analytics 工作区）。
    - TLS（传输层安全性）检查配置。（如果使用 Azure Key Vault、证书和托管标识。）
    - **公共 IP 控制。** 评估依赖 Azure 防火墙公共 IP 的任何外部标识是否保持固定和受信任。
- Azure 防火墙标准层和高级层具有以下依赖项，你可能需要在目标区域中部署这些依赖项：
    - Azure 虚拟网络
    - （如果使用）Log Analytics
- 如果使用 Azure 防火墙高级层的 TLS 检查功能，则还需要在目标区域中部署以下依赖项：
    - Azure Key Vault
    - Azure 托管标识

停机时间

要了解可能涉及的故障时间，请参阅面向 Azure 的云采用框架：选择重定位方法。

迁移步骤

步骤 1: 创建目标区域的资源

1. 在目标区域创建一个新的虚拟网络（VNet）。
2. 在新的 VNet 中配置所需的子网，包括 AzureFirewallSubnet。

步骤 2: 创建新的 Azure Firewall

1. [可选] 如果原有 Azure 防火墙使用的是经典规则。可以使用 Azure PowerShell 迁移 Azure 防火墙中的现有经典规则以创建策略。有关详细信息，请参阅 使用 PowerShell 将 Azure 防火墙配置迁移到 Azure 防火墙策略
2. 如果已经使用了 Azure 防火墙策略，可以使用 Azure PowerShell 迁移现有策略；或者通过 Azure Portal 选择要迁移的 Azure 防火墙策略，点击**导出模板**的方式保存策略，然后重新部署在新区域。

Redeploy-Policy.ps1 是将现有策略重新部署到新区域的 Azure PowerShell 脚本。

用法示例：

```
.\Redeploy-Policy.ps1 `
  -PolicyId <ReourceId> `
  -TargetResourceGroup target-resource-group `
  -NewPolicyName new-policy-name `
  -Location chinanorth3 `
  -SkuTier Standard
```

重要

脚本不迁移威胁情报和 SNAT 专用范围设置。 需要先记下这些设置，然后再手动进行迁移。此脚本仅为示例，请勿直接用于正式环境的迁移。

此脚本需要最新 Azure PowerShell。 运行 Get-Module -ListAvailable Az，查看已安装哪些版本。 如果需要安装，请参阅安装 Azure PowerShell 模块。

```
param (
    # Resource ID of the original Azure firewall policy.
    [Parameter(Mandatory=$true)]
    [string]
    $PolicyId,

    # Target resource group for the new policy.
    [Parameter(Mandatory=$true)]
    [string]
    $TargetResourceGroup,

    # New name for the Azure firewall policy.
    [Parameter(Mandatory=$true)]
    [string]
    $NewPolicyName,

    # Location for the new Azure firewall policy.
    [Parameter(Mandatory=$true)]
    [string]
    $Location,
```

```
    # SKU Tier for the new Azure firewall policy.
    [Parameter(Mandatory=$false)]
    [string]
    $SkuTier = "Premium"
)

$ErrorActionPreference = "Stop"

function EnsureAzureChinaLogin {
    Write-Host "Checking Azure login status"
    try {
        $account = Get-AzContext
        if ($null -eq $account) {
            throw "Not logged in"
        }
        Write-Host "Already logged in as: $($account.Account)"
    }
    catch {
        Write-Host "Not logged in. Logging in to Azure China..."
        Connect-AzAccount -Environment AzureChinaCloud
        $account = Get-AzContext
        if ($null -eq $account) {
            Write-Host "Login failed. Please check your credentials and try again."
            exit(1)
        }
        Write-Host "Logged in successfully as: $($account.Account)"
    }
}

function CreateNewPolicy {
    [CmdletBinding()]
    param (
        [Parameter(Mandatory=$true)]
        [Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicy]
        $OriginalPolicy,
        [Parameter(Mandatory=$true)]
        [string]
        $NewPolicyName,
        [Parameter(Mandatory=$true)]
        [string]
        $TargetResourceGroup,
        [Parameter(Mandatory=$true)]
        [string]
        $Location,
        [Parameter(Mandatory=$true)]
        [string]
        $SkuTier
    )
```

```
    $NewPolicyParameters = @{
        Name = $NewPolicyName
        ResourceGroupName = $TargetResourceGroup
        Location = $Location
        ThreatIntelMode = $OriginalPolicy.ThreatIntelMode
        ThreatIntelWhitelist = $OriginalPolicy.ThreatIntelWhitelist
        PrivateRange = $OriginalPolicy.PrivateRange
        DnsSetting = $OriginalPolicy.DnsSettings
        SqlSetting = $OriginalPolicy.SqlSetting
        ExplicitProxy  = $OriginalPolicy.ExplicitProxy
        DefaultProfile  = $OriginalPolicy.DefaultProfile
        Tag = $OriginalPolicy.Tag
        SkuTier = $SkuTier
    }

    Write-Host "Creating new policy"
    $newPolicy = New-AzFirewallPolicy @NewPolicyParameters

    Write-Host "Populating rules in new policy"
    foreach ($ruleCollectionGroup in $OriginalPolicy.RuleCollectionGroups) {
        $ruleResource = Get-AzResource -ResourceId $ruleCollectionGroup.Id
        $ruleToTransfom = Get-AzFirewallPolicyRuleCollectionGroup -AzureFirewallPolicy $OriginalPolicy -Name $ru
leResource.Name
        $ruleCollectionGroup = @{
            FirewallPolicyObject = $newPolicy
            Priority = $ruleToTransfom.Properties.Priority
            Name = $ruleToTransfom.Name
        }

        if ($ruleToTransfom.Properties.RuleCollection.Count) {
            $ruleCollectionGroup["RuleCollection"] = $ruleToTransfom.Properties.RuleCollection
        }

        Set-AzFirewallPolicyRuleCollectionGroup @ruleCollectionGroup
    }

    return $newPolicy
}

function ValidateAzNetworkModuleExists {
    Write-Host "Validating needed module exists"
    $networkModule = Get-InstalledModule -Name "Az.Network" -MinimumVersion 4.5 -ErrorAction SilentlyConti
nue
    if ($null -eq $networkModule) {
        Write-Host "Please install Az.Network module version 4.5.0 or higher, see instructions: https://github.com/Az
ure/azure-powershell#installation"
        exit(1)
```

```
    }
    $resourceModule = Get-InstalledModule -Name "Az.Resources" -MinimumVersion 4.2 -ErrorAction SilentlyCon
tinue
    if ($null -eq $resourceModule) {
        Write-Host "Please install Az.Resources module version 4.2.0 or higher, see instructions: https://github.com/
Azure/azure-powershell#installation"
        exit(1)
    }
    Import-Module Az.Network -MinimumVersion 4.5.0
    Import-Module Az.Resources -MinimumVersion 4.2.0
}

EnsureAzureChinaLogin
ValidateAzNetworkModuleExists
$originalPolicy = Get-AzFirewallPolicy -ResourceId $PolicyId
$newPolicy = CreateNewPolicy -OriginalPolicy $originalPolicy -NewPolicyName $NewPolicyName -TargetResourc
eGroup $TargetResourceGroup -Location $Location -SkuTier $SkuTier

Write-Host "Migration complete. New policy created: $($newPolicy.Name)" -ForegroundColor Green
```

3. 在目标区域中创建一个新的 Azure Firewall 实例，并选择迁移后的 Azure 防火墙策略

步骤 3: 测试和验证

1. 确保新的 Azure Firewall 实例已成功创建并配置。
2. 进行连通性测试以验证防火墙规则是否正确应用。
3. 确认日志记录和监控设置是否正常工作。

步骤 4: 迁移流量

1. 更新相关的路由表和网络安全组（NSG）以指向新的 Azure Firewall 实例。
2. 逐步切换流量到新的防火墙，以确保没有中断。

步骤 5: 清理旧资源

1. 在确认新的 Azure Firewall 工作正常后，可以删除旧的 Azure Firewall 实例。
2. 清理旧区域中不再使用的资源以节省成本。

注意事项

- 确保在非高峰时段执行迁移，以减少对业务的影响。
- 在迁移过程中，密切监控网络流量和日志，确保没有问题。
- 如果遇到任何问题，可以随时回滚到原来的 Azure Firewall 实例。

相关参考文档

- Azure Firewall 文档
- Azure CLI 文档
- Azure 网络安全组 (NSG) 文档
- Azure 路由表 文档

通过以上步骤，您可以顺利地将 Azure Firewall 从一个区域迁移到另一个区域。如有任何问题，请参考上述文档或联系 Azure 支持团队。

迁移 Azure Key Vault

目录

- 简介
- 先决条件
- 注意事项
  - 服务终结点注意事项
  - 专用终结点注意事项
  - 专用终结点 DNS 集成注意事项
- 准备工作
- 迁移步骤
  - 停止应用程序
  - 备份 Key Vault
  - 在目标区域创建 Key Vault
  - 恢复 Key Vault 数据
  - 更新应用程序配置
  - 验证与测试
  - 清理资源
- 总结

简介

本手册旨在指导如何将 Azure Key Vault （密钥保管库）从一个区域迁移到另一个区域，包括在中国区域间的操作。我们将使用 Azure CLI 工具，并详细介绍每个步骤，确保数据完整性和服务的最小中断。

先决条件

- 验证 Azure 订阅是否允许在目标区域中创建密钥保管库。
- 通过密钥保管库使用的所有 Azure 服务创建依赖项映射。 对于重定位范围内的服务，必须选择适当的重定位策略。
- 根据密钥保管库设计，可能需要在目标区域中部署和配置虚拟网络。
- 创建密钥、机密和证书，需要将用户添加到 “Key Vault Contributor” 角色。
- 记录并计划在目标区域的密钥保管库中重新配置：

- 访问策略和网络配置设置。
- 软删除和清除保护。
- 自动轮换设置。

注意事项

服务终结点注意事项

通过 Azure Key Vault 的虚拟网络服务终结点可将访问限制为指定虚拟网络。 此外，还可通过这些终结点将访问限制为一系列 IPv4（Internet 协议版本 4）地址范围。 任何从外部连接到密钥保管库的用户都无法访问这些资源。 如果在密钥保管库资源的源区域中配置了服务终结点，则需要在目标区域中执行相同的操作。

若要成功在目标区域中重新创建密钥保管库，必须事先创建 VNet 和子网，然后才能进行实际重新创建。

专用终结点注意事项

Azure 专用链接提供从虚拟网络到 Azure 平台即服务 (PaaS)、客户拥有的服务或 Microsoft 合作伙伴服务的专用连接。 专用链接简化了网络体系结构，并通过消除数据在公共 Internet 上的暴露来保护 Azure 中终结点之间的连接。

若要成功在目标区域中重新创建密钥保管库，必须事先创建 VNet 和子网，然后才能进行实际重新创建。

专用终结点 DNS 集成注意事项

请务必正确配置 DNS 设置，将专用终结点 IP 地址解析为连接字符串的完全限定的域名 (FQDN)。

现有 Microsoft Azure 服务可能已有针对公共终结点的 DNS 配置。 必须替代此配置才能使用专用终结点进行连接。

与专用终结点关联的网络接口包含配置 DNS 所需的信息。 网络接口信息包括专用链接资源的 FQDN 和专用 IP 地址。

可使用以下选项来配置专用终结点的 DNS 设置：

- **使用主机文件（仅推荐用于测试）。** 可以使用虚拟机上的主机文件来替代 DNS。
- **使用专用 DNS 区域。** 你可使用专用 DNS 区域来替代专用终结点的 DNS 解析。 可将专用 DNS 区域链接到你的虚拟网络，以解析特定域。
- **使用 DNS 转发器（可选）。** 你可使用 DNS 转发器来替代专用链接资源的 DNS 解析。 创建 DNS 转发规则，以在虚拟网络中托管的 DNS 服务器上使用专用 DNS 区域。

准备工作

在开始之前，请确保您具备以下条件：

1. 一个有效的 Azure 订阅。
2. 源区域和目标区域的权限。
3. 已安装和配置好的 Azure CLI。
4. 确保您的 Key Vault 没有任何正在进行的操作，并且数据已经备份。

迁移步骤

停止应用程序

首先，停止所有正在使用 Key Vault 的应用程序，以确保在迁移过程中 Key Vault 数据不发生变化。

备份 Key Vault

1. 登录 Azure 门户。
2. 导航到需要迁移的 Key Vault（密钥保管库）。
3. 在左侧导航栏"对象"部分，选择"密钥"。
4. 在右侧列表点击需要备份"密钥"所在的行。
5. 在密钥明细信息页面，点击"下载备份"，并保存备份文件。
6. "机密"和"证书"备份操作参照上述步骤。

使用 Azure CLI 备份现有 Key Vault 的所有密钥、机密和证书。

```
# 备份所有密钥
az keyvault key backup `
--vault-name <SourceKeyVaultName> `
--name <KeyName> `
--file <KeyBackupFilePath>

# 备份所有机密
az keyvault secret backup `
--vault-name <SourceKeyVaultName> `
--name <SecretName> `
--file <SecretBackupFilePath>

# 备份所有证书
az keyvault certificate backup `
--vault-name <SourceKeyVaultName> `
--name <CertificateName> `
--file <CertificateBackupFilePath>
```

在目标区域创建 Key Vault

1. 在 Azure 门户中，导航到“创建资源”。
2. 搜索并选择“Key Vault”。
3. 填写创建 Key Vault 的基本信息，并选择目标区域（即迁入区域）。
4. 完成创建，并等待资源部署完成。
5. 配置 Key Vault 的基于角色的访问控制或访问策略。

使用 Azure CLI 在目标区域创建一个新的 Key Vault。

```
# 创建 Key Vault
az keyvault create `
--name <TargetKeyVaultName> `
--resource-group <TargetResourceGroupName> `
--location <TargetRegion>
```

恢复 Key Vault 数据

1. 导航到新建的 Key Vault（密钥保管库）。
2. 在左侧导航栏“对象”部分，选择“密钥”。
3. 在右侧上方点击“还原备份”按钮。
4. 选择对应备份文件，等待系统还原密钥。
5. “机密”和“证书”备份恢复操作参照上述步骤。

使用 Azure CLI 将备份的数据恢复到目标区域的新 Key Vault 中。

```
# 恢复所有密钥
az keyvault key restore `
--vault-name <TargetKeyVaultName> `
--file <KeyBackupFilePath>
# 恢复所有机密
az keyvault secret restore `
--vault-name <TargetKeyVaultName> `
--file <SecretBackupFilePath>

# 恢复所有证书
az keyvault certificate restore `
--vault-name <TargetKeyVaultName> `
--file <CertificateBackupFilePath>
```

更新应用程序配置

将应用程序配置更新为指向新 Key Vault 并重新启动这些应用程序。

```
# 更新应用程序的连接字符串或配置文件指向新的 Key Vault
# 具体如何更新取决于您的应用程序类型
```

验证与测试

1. 重新启动应用程序，并验证是否正常访问新的 Key Vault。
2. 确保所有的密钥、机密和证书均可以被正确读取和使用。

```
# 例如验证应用程序是否能够正确读取机密
```

清理资源

如果确认新 Key Vault 和应用程序正常运行，可以删除源区域的旧 Key Vault 和相关资源。

```
az keyvault delete `
--name <SourceKeyVaultName> `
--resource-group <SourceResourceGroupName>
```

总结

通过以上步骤，您已经成功将 Azure Key Vault 从一个区域迁移到另一个区域。请确保在迁移过程中仔细检查每一步，以避免数据丢失或服务中断。如果遇到任何问题，可以参考 Azure 官方文档或联系 Azure 技术支持。

了解更多 Azure Key Vault 相关信息，请参考如下文档:

- Azure Key Vault 教程
- Azure Key Vault 概述

如有任何问题，请联系您的 Azure 支持团队。

迁移 Azure Managed Disks

目录

- 简介
- 迁移步骤
  - 步骤 1：获取共享访问签名 URI
  - 步骤 2：复制到存储账户
    - 步骤 2.1：AzCopy
    - 步骤 2.2：Azure CLI
  - 步骤 3：在目标环境中创建新的托管磁盘
  - 步骤 4：创建 VM
- 总结

简介

Azure 托管磁盘通过管理与 VM 磁盘关联的存储帐户，简化了 Azure 基础设施即服务 (IaaS) VM 的磁盘管理。

由于您无法直接访问 .vhd 文件，因此无法直接使用 AzCopy 等工具来复制文件。

本文中提供的解决方法是首先通过获取临时共享访问签名 URI 来导出托管磁盘，然后使用此 URI 下载或复制它，再基于 .Vhd 文件在目标区域中创建新的托管磁盘。

迁移步骤

步骤 1：获取共享访问签名 URI

1. 在门户中，搜索托管磁盘。它与 VM 位于同一资源组中，其资源类型为**磁盘**。
2. 在左侧功能列表中选择**磁盘导出**菜单。您必须先关闭并取消分配 VM，或者取消附加 VM 以完成导出。
3. 定义 URI 到期的时间。默认时间为 3600 秒。
4. 生成一个 URL。
5. 复制该 URL。该 URL 只会在创建后显示一次。

步骤 2：复制到存储账户

有多种方式可以将导出的磁盘复制到目标存储账户中，本文将以 AzCopy 和 Azure CLI 两种方式为例进行介绍，可自行选择使用。

步骤 2.1：AzCopy

使用 AzCopy 将磁盘直接从源环境复制到目标环境的存储账户 Blob 容器中。

有关如何使用 AzCopy ，请参阅 AzCopy 入门。

AzCopy 命令如下：

```
azcopy copy "<源 SAS URI>" "<目标 SAS URI>" --blob-type PageBlob
```

以下是完整的命令示例：

```
azcopy copy
"https://md-fvth500tz1jn.blob.core.chinacloudapi.cn/nd2vhh3qsbn2/abcd?sv=2018-03-28&sr=b&si=08af14df-4aea-444c-89de-06c251f213ae&sig=xxx"
"https://targetstorage.blob.core.chinacloudapi.cn/targetcontainer/newdisk.vhd?sp=rcw&st=2024-09-13T03:16:24Z&se=2024-09-13T11:16:24Z&spr=https&sv=2022-11-02&sr=c&sig=xxx"
--blob-type PageBlob
```

重要事项

- 确保 URI 的有效性和权限设置正确，尤其是在处理 SAS 令牌时。 - 使用 –blob-type PageBlob 是因为托管磁盘通常以页面 Blob 的形式存储。 - 确认源和目标存储账户的网络设置，例如防火墙和虚拟网络配置，以确保 AzCopy 能够成功连接到两者。

步骤 2.2：Azure CLI

使用 Azure CLI 将磁盘直接从源环境复制到目标环境的存储账户 Blob 容器中。

Azure CLI 命令如下：

```
az storage blob copy start
--destination-blob "<目标 VHD 文件名>"
--destination-container "<目标存储账户容器名>"
--account-name "<目标存储账户名>"
--account-key "<目标存储账户 Key>"
--source-uri "<源 SAS URI>"
```

当然，您也可以通过 Azure CLI 完成 步骤 1：获取共享访问签名 URI 中获取 SAS URI 的过程。
如果您想通过脚本自动化迁移大量托管磁盘，这无疑是一种很好的方式。

完整过程及脚本，请看 使用 Azure CLI 将托管磁盘导出/复制到存储帐户。

步骤 3：在目标环境中创建新的托管磁盘

有几种方法可用于创建新的托管磁盘。以下是在 Azure 门户执行该操作的方法： 1. 在门户中，选择**新建 > 托管磁盘 > 创建**。 2. 输入新磁盘的名称。 3. 选择资源组。 4. 在**源类型**下，选择**存储 blob**。然后，从 AzCopy 命令复制目标 URI，或进行浏览以选择目标 URI。 5. 如果复制的是 OS 磁盘，请选择 **OS** 类型。对于其他磁盘类型，请选择**创建**。

步骤 4：创建 VM

如前所述，有多种方法可以使用此新托管磁盘创建 VM。以下是两种选项： * 在门户中，选择磁盘，然后选择**创建 VM**。像往常一样定义 VM 的其他参数。 * 利用 PowerShell 的创建，请参阅从还原磁盘创建 VM。

总结

通过以上步骤，您已经成功将 Azure 托管磁盘从一个区域迁移到另一个区域。

请确保在迁移过程中仔细检查每一步，以避免数据丢失或服务中断。

在生产环境迁移前，请先在测试环境进行测试验证。

如果遇到任何问题，可以参考 Azure 官方文档或联系 Azure 技术支持。

了解更多关于管理 Azure 的托管磁盘，请参考：

- Azure 托管磁盘文档
- 了解如何通过 API 获取共享访问签名 URI，以导出到磁盘。
- 了解如何通过 API 从非托管 blob 创建托管磁盘。

迁移 Azure Storage Account

概述

本章节将指导您如何将 Azure Storage Account 从一个区域迁移到另一个区域。由于 Azure 不支持直接更改存储账户的区域，我们需要通过备份和复制数据来实现迁移。

先决条件

在开始迁移之前，请确保满足以下条件：

- 确保帐户使用的服务和功能在目标区域中受支持。
- 对于预览功能，请确保你的订阅已列入目标区域的允许列表。
- 根据存储帐户部署的不同，在重新定位之前，可能需要在目标区域中部署和配置以下依赖资源：
    - 虚拟网络、网络安全组和用户定义的路由
    - Azure Key Vault
    - Azure 自动化
    - 公共 IP
    - Azure 专用链接服务
- 拥有 Azure 订阅和必要的权限。

迁移考虑事项

数据迁移类型

在迁移过程中，您需要考虑以下数据类型：

- **Blob 存储**：用于对象存储。
- **Azure Files**：用于文件共享。
- **Table 存储**：用于 NoSQL 数据存储。
- **Queue 存储**：用于消息队列。

可能的依赖项

确保所有依赖于源存储账户的服务和应用程序都能正确访问新的存储账户。这包括但不限于：

- Azure Web Apps

- Virtual Machines
- Azure Kubernetes Service
- Azure Container Instances
- Azure Functions
- Azure Batch
- Azure Synapse Analytics
- Azure Databricks
- 其他使用存储账户的 Azure 服务

迁移时间

- **规划窗口**：选择一个对业务影响最小的时间段进行迁移操作，建议在非高峰时段或维护窗口期间进行。
- **预估时间**：根据存储账户中数据量的大小，预估整个迁移过程所需时间。大规模数据迁移可能需要数小时到数天不等。

停机影响

- **计划停机**：如果允许停机迁移，可以在迁移期间暂停或关闭依赖该存储账户的所有服务，以减少数据不一致的风险。
- **最小化停机**：对于需要保持业务连续性的场景，需设计迁移策略以确保尽可能小的停机时间，如使用读写权限切换或设置临时转发机制。

不停机的数据增量迁移

- **初始同步**：首先完成一次全量数据的备份和复制到目标区域的存储账户。
- **增量同步**：在全量迁移后，使用如 Azure Data Factory、AzCopy 的 `/Sync` 参数或 Event Grid 与函数触发的复制逻辑来捕捉并迁移增量数据变化，确保迁移过程中新产生的数据不会丢失。
- **最终一致性**：确定一个最终切换点，停止源存储账户上的写操作，执行最后一次增量同步，然后将所有服务指向新的存储账户。

测试与验证

- **校验和对比**：在迁移前后，利用存储服务提供的校验和功能（如 Blob 的 MD5 或 File 的 Content-MD5）来验证数据块的完整性，确保源存储账户与目标存储账户中的数据完全一致。
- **样本验证**：随机选取部分数据进行详细比对，包括元数据、访问控制列表（ACL）等，确保迁移过程中这些信息未被遗漏或修改。
- **全体数据扫描**：对于重要且数据量可管理的存储，可以进行全体数据的逐项比对，确保无一遗漏。

成本考量

评估迁移过程中和迁移后可能产生的额外费用，包括数据网络传输费、存储费、以及可能的计算资源费用（用于数据处理和迁移）。

迁移方案

Storage Account

- Azure Storage Account - 将 Azure 存储帐户重新定位到另一个区域

Blob 存储

对于 Blob 容器

- Azure Blob - 使用 AzCopy 在 Azure 存储帐户之间复制 Blob
- 使用 Azure 数据工厂向/从 Azure Blob 存储复制数据

对于 Azure 非托管磁盘

- 根据最佳做法，Azure 建议将非托管磁盘转换为托管磁盘。请了解 在 2025 年 9 月 30 日前迁移 Azure 非托管磁盘 的相关说明。
- 请参考 将 Azure VM 迁移到 Azure 中的托管磁盘

Azure Data Lake Storage Gen2

- 可以参考 AzCopy 进行存储帐户之间复制
- 可以参考 使用 Azure 数据工厂或 Azure Synapse Analytics 复制和转换 Azure Data Lake Storage Gen2 中的数据

Azure Files

- Azure Files - 将文件从一个 SMB Azure 文件共享迁移到另一个 SMB Azure 文件共享
- 使用 Azure 数据工厂从/向 Azure 文件存储复制数据

Table 存储

根据最佳做法，我们建议您将 Table 存储 迁移到 Azure Cosmos DB for Table 帐户中。如果需要继续使用 Table 存储，也可以参考后续的步骤进行数据的迁移。

- 将数据迁移到 Azure Cosmos DB for Table 帐户
- 使用 Azure 数据工厂向/从 Azure 表存储复制数据

使用 AZCopy 进行复制

目前已知的最后支持 Table 存储复制的是 AZCopy V8 版本，之后的版本 Azure Table 存储的复制功能已不再受支持。请参考下文的 Azure Storage Explorer 迁移方法。

使用 Azure Storage Explorer 进行迁移

前提条件

- 已安装最新版本的 Azure Storage Explorer

步骤 1：连接到源和目标存储帐户

1. 打开 Azure Storage Explorer。
2. 在左侧的资源管理器中，点击“添加帐户”或“连接到 Azure 存储”。
3. 择适当的连接方法（如通过 Azure Active Directory、使用存储帐户名称和密钥等）。
4. 依次连接到源存储帐户和目标存储帐户。

步骤 2：迁移 Table 数据

1. 在 Azure Storage Explorer 中，展开源存储帐户，找到要迁移的 Table。
2. 右键点击要迁移的 Table，选择“复制表”。
3. 展开目标存储帐户，存储账户下 Tables。
4. 右键点击 Tables，选择“粘贴表”。
5. 监视活动内的提示信息，直到出现类似如下信息

已成功将表“source/tableName”复制到“target/tableName”；已复制 n 个实体

Queue 存储

在迁移 Queue 存储时，建议采用在新区域创建新队列，并切换应用程序将消息写入到新队列中。等待旧队列数据完全被消耗，将应用程序读取队列的配置切换到新队列。

相关参考文档

- 选择 Azure 数据传输解决方案
- 通过 Azure 存储优化 AzCopy 的性能
- 使用 Azure CLI 管理存储帐户本地用户
- 将自定义域映射到 Azure Blob 存储终结点

迁移 Azure 流分析作业

要跨 Azure 区域迁移 Azure 流分析服务，最简单的方法是使用适用于 Azure 流分析的 Visual Studio Code 工具将作业复制到其他区域。 > **注意:**
> Visual Studio 的 ASA（Azure Stream Analytics） 工具扩展不再进行维护。 建议使用 Visual Studio Code 中的 ASA 工具扩展进行此项任务。

您还可以使用 Azure 门户或使用 PowerShell 在目标 Azure 区域中手动重新搭建服务。流分析作业的入口和出口源可以位于任何区域。

您可以参考如下步骤借助 Visual Studio Code 工具进行 zure 流分析的迁移工作。

准备工作

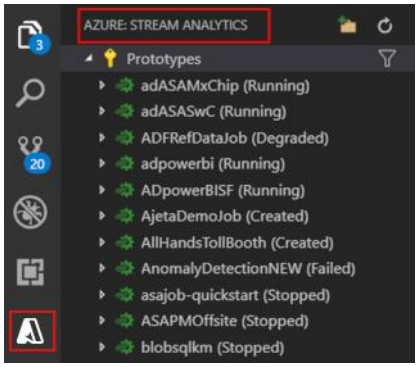
在开始之前，请确保您已经具备以下条件：

1. 一个有效的 Azure 订阅。
2. 源区域和目标区域的权限。
3. 安装 Visual Studio Code。
4. 安装适用于 Visual Studio Code 的 Azure 流分析扩展。
5. 使用 Visual Studio Code 登录中国区 Azure.

迁移步骤

从 Visual Studio Code 中显示流分析作业

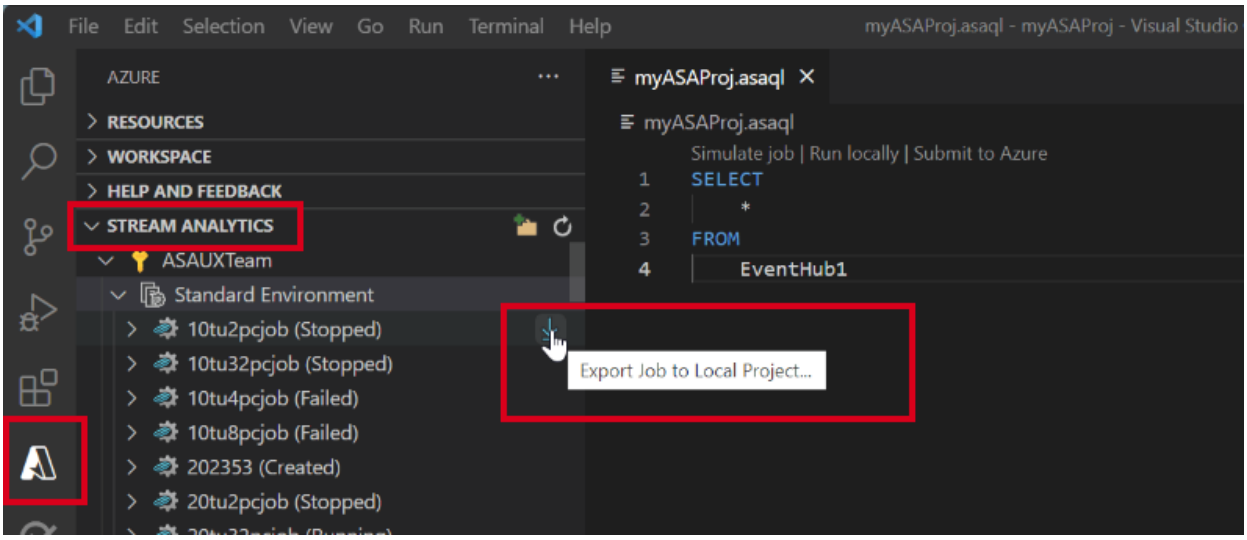
选择 Visual Studio Code 活动栏上的“Azure”图标，然后展开“流分析”节点。 找到需要迁移的作业。



打开流分析资源管理器

导出配置和状态

若要将作业导出到本地项目，请在 Visual Studio Code 的流分析资源管理器中找到要导出的作业。 然后为导出的项目选择一个文件夹。



在 Visual Studio Code 中找到 ASA 作业

项目会导出到所选文件夹并添加到当前工作区。

创建目标区域资源组

在目标区域创建资源组。

复制输入和输出资源

确保源区域和目标区域的输入和输出资源一致。具体的步骤取决于您使用的输入和输出类型，例如 Blob 存储，事件中心，SQL 数据库等。根据实际情况，创建这些资源。

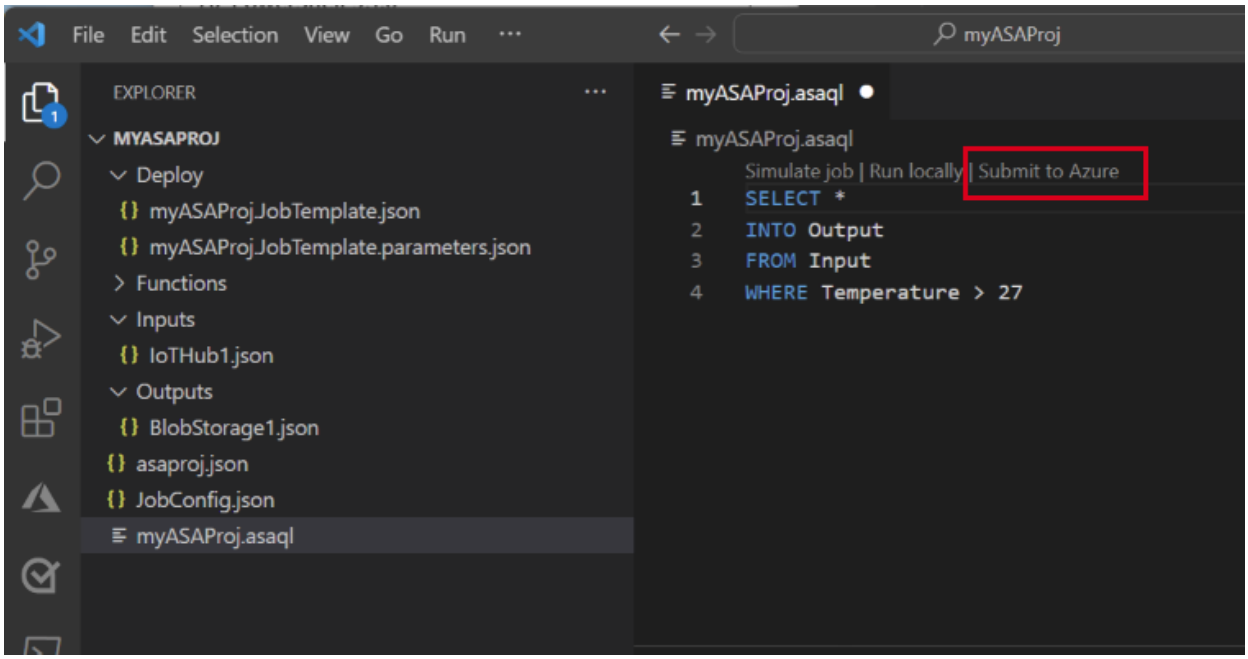
创建新的 Azure 流分析作业

在目标区域创建新的 Azure 流分析作业。如果您希望在导入过程中在目标创建 Azure 流分析作业，您可以跳过此步骤，进入下面步骤。

导入配置到目标端

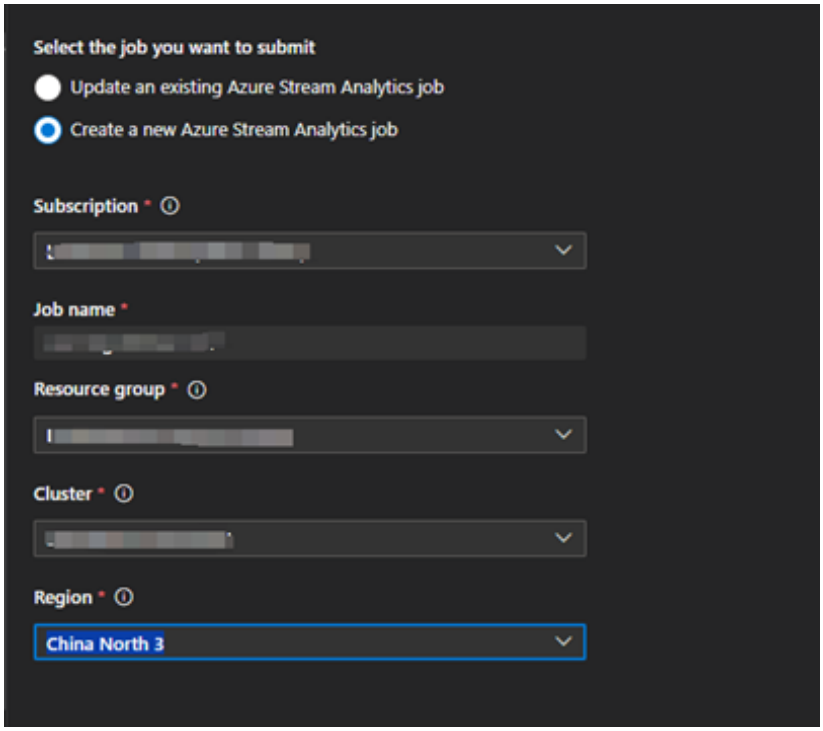
在 Visual Studio Code 中的查询编辑器中找到前面步骤导出的项目文件，点击(*.asaql)文件，并选择“Submit to Azure”，然后按照说明进行操作。

在此操作中，您可以将配置导入到目标已经存在的 Azure 流分析作业，或者选择创建一个新的 Azure 流分析作业并导入配置。



导入配置

如果您选择创建一个新的 Azure 流分析作业并导入配置，注意选择您的目标区域。



选择 Job

停止原有的 Azure 流分析作业

在上述相关工作完成，并对目标区域相关配置检查更新完成后，可以通过 Azure 门户停止原有区域的 Azure 流分析作业，并准备启动目标区域 Azure 流分析作业。

启动新的 Azure 流分析作业

启动新的 Azure 流分析作业，开始数据处理。

验证与测试

1. 通过 Azure 门户或 Azure CLI 检查新作业的状态和运行情况。
2. 确认输入和输出数据流是否正常处理。
3. 监控作业一段时间，确保数据处理没有任何错误或丢失。

清理资源

如果确认新的 Azure 流分析作业运行正常，可以删除源区域的旧作业和相关资源。

总结

通过以上步骤，您已经成功将 Azure 流分析作业从一个区域迁移到另一个区域。请确保在迁移过程中仔细检查每一步，以避免数据丢失或服务中断。如果遇到任何问题，可以参考 Azure 官方文档或联系 Azure 技术支持。

有关更多信息： * 通过完成流分析教程来刷新您的知识。 * 查阅流分析概述。 * 了解如何使用 PowerShell 创建流分析作业。

如有任何问题，请联系您的 Azure 支持团队。

迁移 Azure Synapse Analytics 工作区

本文是一篇分步指南，介绍如何将 Azure Synapse Analytics 工作区从一个 Azure 区域移到另一个区域。

备注:
本文中的步骤实际上并未移动工作区。 这些步骤展示了如何利用源区域中的 Azure Synapse Analytics 专用 SQL 池的备份以及源区域中的脚本等文件，在新的区域中创建新工作区，以实现跨区域的迁移工作

准备工作

在开始之前，请确保您已经具备以下条件：

1. 一个有效的 Azure 订阅。
2. 源区域和目标区域的权限
3. 将源区域 Azure Synapse 工作区与 Azure DevOps 或 GitHub 集成。 有关详细信息，请参阅 Synapse Studio 中的源代码管理。
4. 在执行脚本的服务器上安装 Azure PowerShell 和 Azure CLI 模块。在执行脚本的服务器上安装 Azure PowerShell 和 Azure CLI 模块。
5. 确保在目标区域中重新创建所有从属服务（例如 Azure 机器学习、Azure 存储和 Azure 专用链接中心），或将其移到目标区域（如果服务支持区域移动）。
6. 将 Azure 存储移到其他区域。 有关详细信息，请参阅将 Azure 存储帐户移到另一区域。
7. 确保源区域和目标区域工作区中的专用 SQL 池名称和 Apache Spark 池名称相同。

将 Azure Synapse 工作区移到另一个区域的步骤

将 Azure Synapse 工作区从一个区域移到另一个区域是一个多步骤过程。 下面是概要步骤：

1. 在目标区域中创建一个新的 Azure Synapse 工作区，同时创建一个 Spark 池，其配置与源区域工作区中使用的配置相同。
2. 使用还原点或异地备份将专用 SQL 池还原到目标区域。
3. 在新的逻辑 SQL Server 上重新创建所有必需的登录名。
4. 创建无服务器 SQL 池和 Spark 池数据库和对象。
5. 如果要使用 Azure DevOps 发布管道来部署项目，请将 Azure DevOps 服务主体添加到 Azure Synapse 基于角色的访问控制 (RBAC) Synapse 项目发布者角色。
6. 将代码项目（SQL 脚本、笔记本）、链接服务、管道、数据集、Spark 作业定义触发器和凭据从 Azure DevOps 发布管道部署到目标区域 Azure Synapse 工作区。
7. 将 Microsoft Entra 用户或组添加到 Azure Synapse RBAC 角色。 如果要使用托管标识进行身份验证，请授权存储 Blob 参与者访问 Azure 存储和 Azure Key Vault 上系统分配的托管标识 (SA-MI)。

8. 在默认附加存储或包含要使用无服务器 SQL 池查询的数据的存储帐户上，向所需的 Microsoft Entra 用户授予“存储 Blob 读取者”或“存储 Blob 参与者”角色。
9. 重新创建自承载集成运行时 (SHIR)。
10. 在目标 Azure Synapse 工作区中手动上传所有必需的库和 jar。
11. 如果工作区部署在托管虚拟网络中，则创建所有托管专用终结点。
12. 测试目标区域中的新工作区，并更新指向源区域工作区的所有 DNS 条目。
13. 如果在源工作区中创建了专用终结点连接，请在目标区域工作区中也创建一个。
14. 在对源区域中的工作区进行全面测试并将所有连接路由到目标区域工作区之后，可以删除源区域中的工作区。

准备

步骤 1：在目标区域中创建 Azure Synapse 工作区

在本部分中，你将使用 Azure PowerShell、Azure CLI 和 Azure 门户创建 Azure Synapse 工作区。 你将创建一个资源组和一个 Azure Data Lake Storage Gen2 帐户，该帐户将作为 PowerShell 脚本和 CLI 脚本的一部分，用作工作区的默认存储。 若要自动执行部署过程，请从 DevOps 发布管道调用这些 PowerShell 或 CLI 脚本。

Azure 门户

若要从 Azure 门户创建工作区，请按照快速入门：创建 Synapse 工作区中的步骤操作。

Azure PowerShell

以下脚本使用 New-AzResourceGroup 和 New-AzSynapseWorkspace cmdlet 创建资源组和 Azure Synapse 工作区。

请注意首先使用 Azure PowerShell 连接和登录 China Azure Cloud。若要了解如何在不同 Azure 云之间切换，请参阅 Sign in to Azure PowerShell interactively。

创建资源组

PowerShell

```
$storageAccountName= "<YourDefaultStorageAccountName>"
$resourceGroupName="<YourResourceGroupName>"
$regionName="<YourTargetRegionName>"
$containerName="<YourFileSystemName>" # This is the file system name
$workspaceName="<YourTargetRegionWorkspaceName>"

$sourcRegionWSName="<Your source region workspace name>"
$sourceRegionRGName="<YourSourceRegionResourceGroupName>"
```

```
$sqlUserName="<SQLUserName>"
$sqlPassword="<SQLStrongPassword>"

$sqlPoolName ="<YourTargetSQLPoolName>" #Both Source and target workspace SQL pool name will be same
$sparkPoolName ="<YourTargetWorkspaceSparkPoolName>"
$sparkVersion="2.4"

New-AzResourceGroup -Name $resourceGroupName -Location $regionName
```

创建 Data Lake Storage Gen2 帐户

PowerShell

```
#If the Storage account is already created, then you can skip this step.
New-AzStorageAccount -ResourceGroupName $resourceGroupName `
 -Name $storageAccountName `
 -Location  $regionName `
 -SkuName Standard_LRS `
 -Kind StorageV2 `
 -EnableHierarchicalNamespace $true
```

创建 Azure Synapse 工作区

PowerShell

```
$password = ConvertTo-SecureString $sqlPassword -AsPlainText -Force
$creds = New-Object System.Management.Automation.PSCredential ($sqlUserName, $password)

New-AzSynapseWorkspace -ResourceGroupName $resourceGroupName `
 -Name $workspaceName -Location $regionName `
 -DefaultDataLakeStorageAccountName $storageAccountName `
 -DefaultDataLakeStorageFilesystem $containerName `
 -SqlAdministratorLoginCredential $creds
```

若要使用托管虚拟网络创建工作区，请向该脚本添加额外的参数“ManagedVirtualNetwork”。 若要详细了解可用的选项，请参阅托管虚拟网络配置。

PowerShell

```
#Creating a managed virtual network configuration
$config = New-AzSynapseManagedVirtualNetworkConfig -PreventDataExfiltration -AllowedAadTenantIdsForLinking ContosoTenantId

#Creating an Azure Synapse workspace
New-AzSynapseWorkspace -ResourceGroupName $resourceGroupName `
 -Name $workspaceName -Location $regionName `
 -DefaultDataLakeStorageAccountName $storageAccountName `
 -DefaultDataLakeStorageFilesystem $containerName `
```

```
 -SqlAdministratorLoginCredential $creds `
 -ManagedVirtualNetwork $config
```

Azure CLI

此 Azure CLI 脚本将创建资源组、Data Lake Storage Gen2 帐户和文件系统。 然后，创建 Azure Synapse 工作区。

请注意首先使用 Azure CLI 连接和登录 China Azure Cloud。若要了解如何在不同 Azure 云之间切换，请参阅 Azure 云管理与 Azure CLI。

创建资源组

Azure CLI

```
az group create --name $resourceGroupName --location $regionName
```

创建 Data Lake Storage Gen2 帐户

以下脚本会创建存储帐户和容器。

Azure CLI

```
# Checking if name is not used only then creates it.
$StorageAccountNameAvailable=(az storage account check-name --name $storageAccountName --subscription $subscriptionId | ConvertFrom-Json).nameAvailableif($StorageAccountNameAvailable){Write-Host "Storage account Name is available to be used...creating storage account"

#Creating a Data Lake Storage Gen2 account
$storgeAccountProvisionStatus=az storage account create `
 --name $storageAccountName `
 --resource-group $resourceGroupName `
 --location $regionName `
 --sku Standard_GRS `
 --kind StorageV2 `
 --enable-hierarchical-namespace $true

($storgeAccountProvisionStatus| ConvertFrom-Json).provisioningState}else{    Write-Host "Storage account Name is NOT available to be used...use another name --    exiting the script..."
   EXIT}

#Creating a container in a Data Lake Storage Gen2 account

$key=(az storage account keys list -g $resourceGroupName -n $storageAccountName|ConvertFrom-Json)[0].value

$fileShareStatus=(az storage share create --account-name $storageAccountName --name $containerName --account-key $key)if(($fileShareStatus|ConvertFrom-Json).created -eq "True"){    Write-Host f"Successfully created th
```

```
e fileshare - '$containerName'"
}
```

创建 Azure Synapse 工作区

Azure CLI

```
az synapse workspace create `
 --name $workspaceName `
 --resource-group $resourceGroupName `
 --storage-account $storageAccountName `
 --file-system $containerName `
 --sql-admin-login-user $sqlUserName `
 --sql-admin-login-password $sqlPassword `
 --location $regionName
```

若要启用托管虚拟网络，请在上述脚本中包含参数 --enable-managed-virtual-network。 有关更多选项，请参阅工作区托管虚拟网络。

Azure CLI

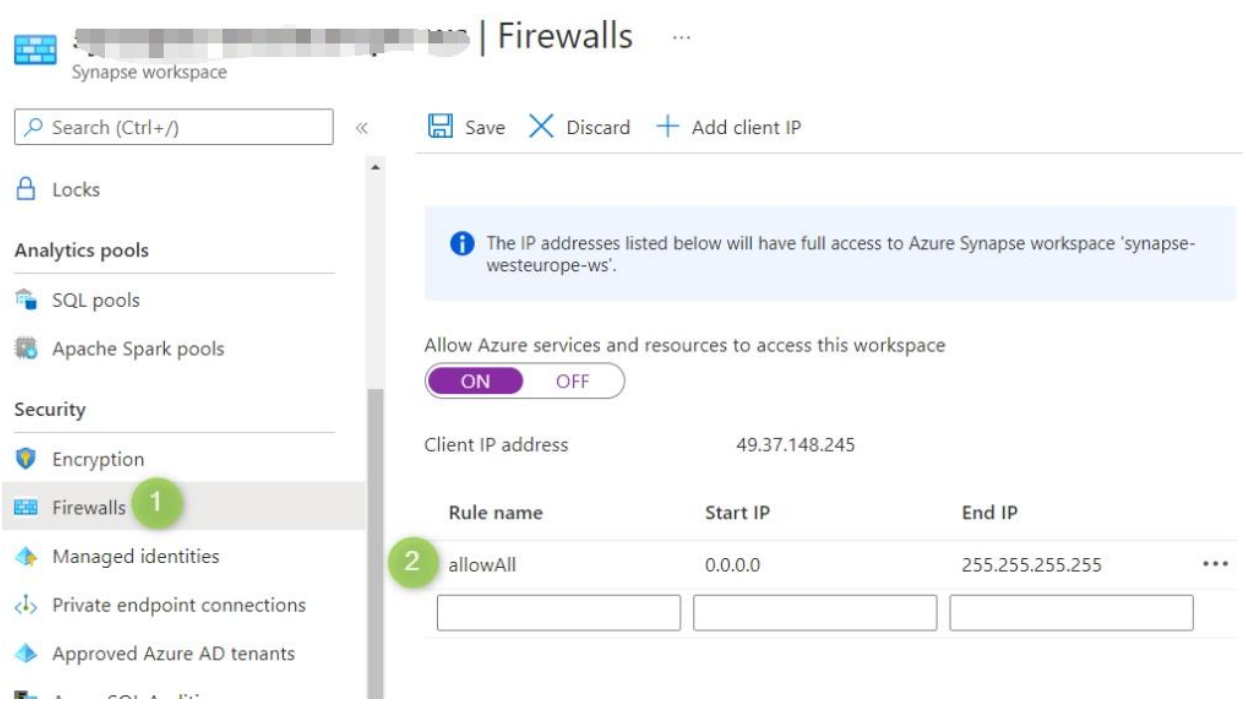
```
az synapse workspace create `
 --name $workspaceName `
 --resource-group $resourceGroupName `
 --storage-account $storageAccountName `
 --file-system $FileShareName `
 --sql-admin-login-user $sqlUserName `
 --sql-admin-login-password $sqlPassword `
 --location $regionName `
 --enable-managed-virtual-network true `
 --allowed-tenant-ids "Contoso"
```

步骤 2：创建 Azure Synapse 工作区防火墙规则

创建工作区后，为工作区添加防火墙规则。 将 IP 限制在一定范围内。 可以从 Azure 门户或者使用 PowerShell 或 CLI 添加防火墙。

Azure 门户

选择防火墙选项并添加 IP 地址范围，如下面的屏幕截图所示。



Azure PowerShell

运行以下 PowerShell 命令，通过指定开始和结束 IP 地址来添加防火墙规则。 根据你的要求更新 IP 地址范围。

PowerShell

```
$WorkspaceWeb = (Get-AzSynapseWorkspace -Name $workspaceName -ResourceGroupName $resourceGroup).ConnectivityEndpoints.Web
$WorkspaceDev = (Get-AzSynapseWorkspace -Name $workspaceName -ResourceGroupName $resourceGroup).ConnectivityEndpoints.Dev

# Adding firewall rules
$FirewallParams = @{ WorkspaceName = $workspaceName
 Name = 'Allow Client IP'
 ResourceGroupName = $resourceGroup
 StartIpAddress = "0.0.0.0"
 EndIpAddress = "255.255.255.255"
}
New-AzSynapseFirewallRule @FirewallParams
```

运行以下脚本以更新工作区的托管标识 SQL 控制设置：

PowerShell

```
Set-AzSynapseManagedIdentitySqlControlSetting -WorkspaceName $workspaceName -Enabled $true
```

Azure CLI

Azure CLI

```
az synapse workspace firewall-rule create --name allowAll --workspace-name $workspaceName `
--resource-group $resourceGroupName --start-ip-address 0.0.0.0 --end-ip-address 255.255.255.255
```

运行以下脚本以更新工作区的托管标识 SQL 控制设置：

Azure CLI

```
az synapse workspace managed-identity grant-sql-access `
--workspace-name $workspaceName --resource-group $resourceGroupName
```

步骤 3：创建 Apache Spark 池

使用源区域工作区中所用的配置来创建 Spark 池。

Azure 门户

若要从 Azure 门户创建 Spark 池，请参阅快速入门：使用 Azure 门户新建无服务器 Apache Spark 池。

你还可以按照快速入门：使用 Synapse Studio 创建无服务器 Apache Spark 池中的步骤，从 Synapse Studio 创建 Spark 池。

Azure PowerShell

以下脚本会创建一个 Spark 池，其中包含两个辅助角色和一个驱动程序节点，以及一个具有 4 个核心和 32 GB RAM 的小型群集大小。 更新值，使其与源区域工作区 Spark 池匹配。

PowerShell

```
#Creating a Spark pool with 3 nodes (2 worker + 1 driver) and a small cluster size with 4 cores and 32 GB RAM.
New-AzSynapseSparkPool `
 -WorkspaceName  $workspaceName `
 -Name $sparkPoolName `
 -NodeCount 3 `
 -SparkVersion $sparkVersion `
 -NodeSize Small
```

Azure CLI

Azure CLI

```
az synapse spark pool create --name $sparkPoolName --workspace-name $workspaceName --resource-group $r
esourceGroupName `
--spark-version $sparkVersion --node-count 3 --node-size small
```

移动

步骤 4：还原专用 SQL 池

从异地冗余备份中还原

若要使用 Azure 门户和 PowerShell 从异地备份中还原专用 SQL 池，请参阅在 Azure Synapse Analytics 中异地还原专用 SQL 池。

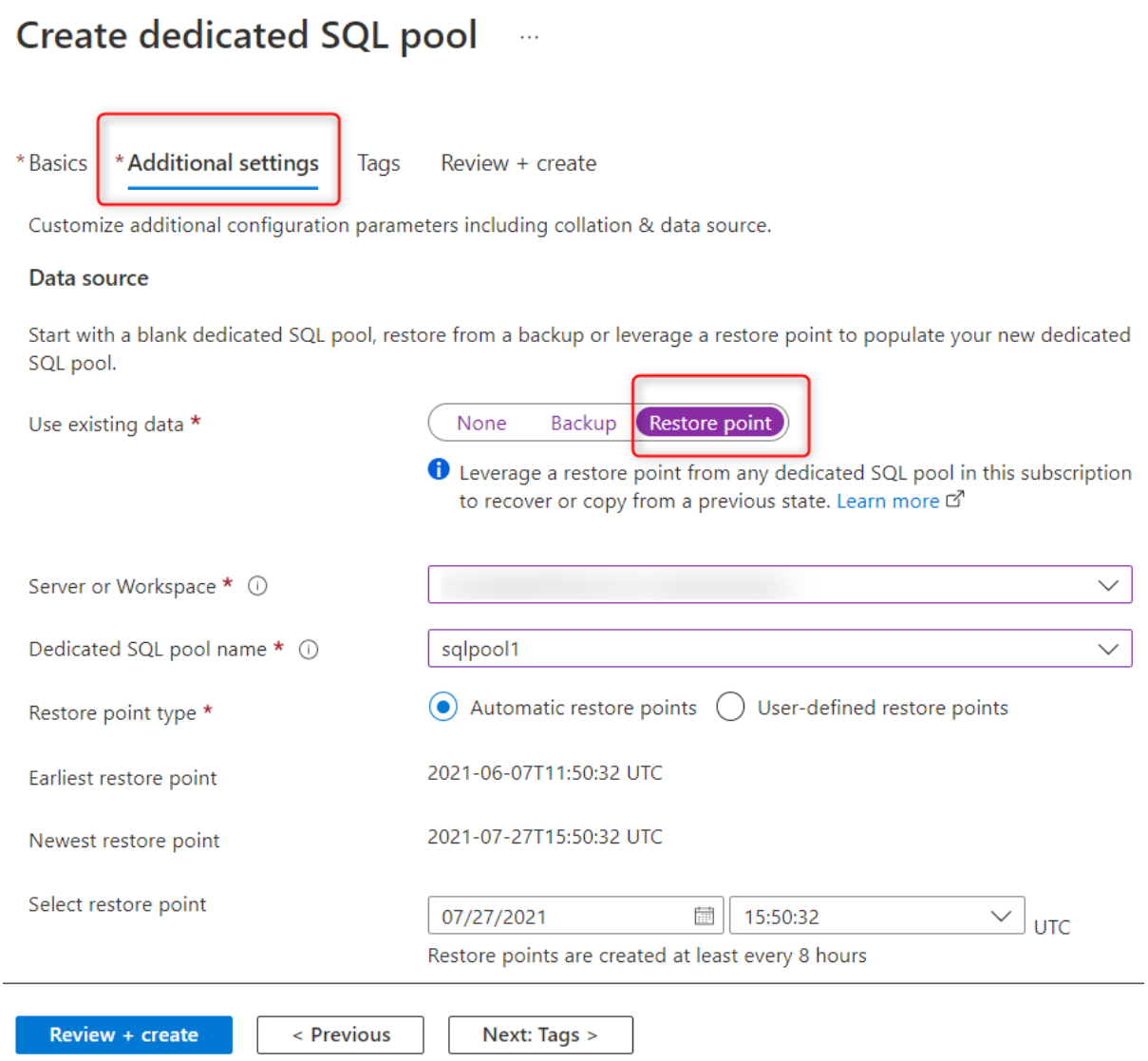
使用源区域工作区专用 SQL 池中的还原点进行还原

使用源区域工作区专用 SQL 池的还原点将专用 SQL 池还原到目标区域工作区。 可以使用 Azure 门户、Synapse Studio 或 PowerShell 从还原点进行还原。 如果源区域不可访问，则无法使用此选项进行还原。

在源区域进行还原点的创建，请参考专用 SQL 池（以前称为 SQL DW）的用户定义还原点。

Synapse Studio

在 Synapse Studio 中，可以使用还原点从订阅中的任何工作区还原专用 SQL 池。 创建专用 SQL 池时，在“其他设置”下，选择“还原点”并选择工作区，如下面的屏幕截图所示。 如果创建了用户定义的还原点，请使用它来还原 SQL 池。 否则，可以选择最新的自动还原点。



还原 SQL 池

Azure PowerShell

运行以下 PowerShell 脚本还原工作区。 此脚本使用源工作区专用 SQL 池中的最新还原点，在目标工作区中还原 SQL 池。 在运行该脚本之前，请将性能级别从 DW100c 更新为所需的值。

重要 两个工作区中的专用 SQL 池名称应该相同。

获取还原点：

PowerShell

```
$restorePoint=Get-AzSynapseSqlPoolRestorePoint -WorkspaceName $sourceRegionWSName -Name $sqlPoolName|Sort-Object  -Property RestorePointCreationDate -Descending `
| SELECT RestorePointCreationDate -ExpandProperty  RestorePointCreationDate -First 1
```

将 Azure Synapse SQL 池资源 ID 转换为 SQL 数据库 ID，因为目前此命令仅接受 SQL 数据库 ID。 例如：

`/subscriptions/<SubscriptionId>/resourceGroups/<ResourceGroupName>/providers/Microsoft.Sql/servers/<WorkspaceName>/databases/<DatabaseName>`

PowerShell

```
$pool = Get-AzSynapseSqlPool -ResourceGroupName $sourceRegionRGName -WorkspaceName $sourcRegionWSName -Name $sqlPoolName
$databaseId = $pool.Id `
  -replace "Microsoft.Synapse", "Microsoft.Sql" `
  -replace "workspaces", "servers" `
  -replace "sqlPools", "databases"

$restoredPool = Restore-AzSynapseSqlPool -FromRestorePoint `
  -RestorePoint $restorePoint `
  -TargetSqlPoolName $sqlPoolName `
  -ResourceGroupName $resourceGroupName `
  -WorkspaceName $workspaceName `
  -ResourceId $databaseId `
  -PerformanceLevel DW100c -AsJob
```

以下命令跟踪还原操作的状态：

```
Get-Job | Where-Object Command -In ("Restore-AzSynapseSqlPool") | `
Select-Object Id,Command,JobStateInfo,PSBeginTime,PSEndTime,PSJobTypeName,Error |Format-Table
```

还原专用 SQL 池后，在 Azure Synapse 中创建所有 SQL 登录名。 若要创建所有登录名，请按照创建登录名中的步骤操作。

如果由于一些特定需求，希望通过将专用 SQL 池中代码和数据对象，分别手工复制到目标区域专用 SQL 池，也可以考虑通过导出数据库对象 DDL，在目标端进行重建。然后通过数据复制将数据复制到目标端，则可以参考如下内容。 * 使用数据工厂自行进行数据迁移，可以参考使用 Azure 数据工厂或 Synapse 管道将数据加载到 Azure Synapse Analytics 中 * 使用 Visual Studio 和 SSDT 连接专用 SQL 池，可以参考使用 Visual Studio 和 SSDT 连接到 Azure Synapse Analytics 中的专用 SQL 池（以前称为 SQL DW）

步骤 5：创建无服务器 SQL 池、Spark 池数据库和对象

你无法备份和还原无服务器 SQL 池数据库和 Spark 池。 作为一种可能的解决方法，你可以：

1. 创建笔记本和 SQL 脚本，其中包含用于重新创建所有所需 Spark 池、无服务器 SQL 池数据库、表、角色和具有所有角色分配的用户的代码。 将这些项目签入 Azure DevOps 或 GitHub。
2. 如果存储帐户名称已更改，请确保代码项目指向正确的存储帐户名称。
3. 创建管道，以特定顺序调用这些代码项目。 在目标区域工作区中执行这些管道时，将在目标区域工作区中创建 Spark SQL 数据库、无服务器 SQL 池数据库、外部数据源、视图、角色以及用户和权限。

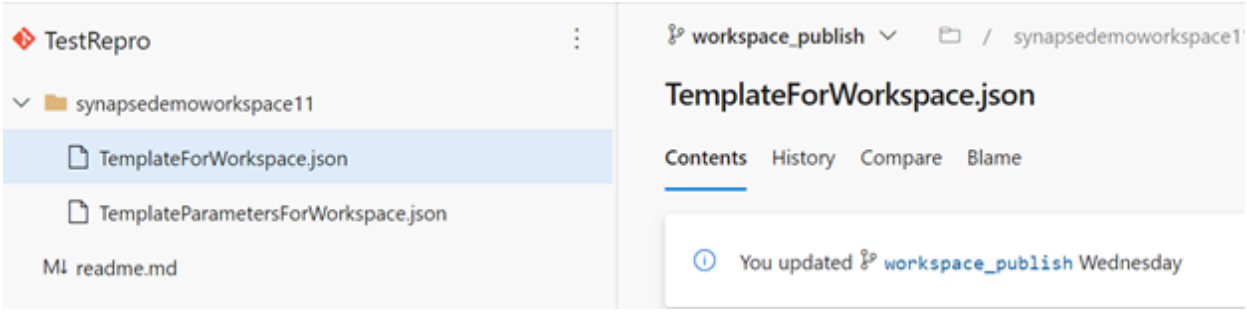
4. 将源区域工作区与 Azure DevOps 集成时，这些代码项目将成为存储库的一部分。 稍后，你可以使用步骤 6 中提到的 DevOps 发布管道将这些代码项目部署到目标区域工作区。
5. 在目标区域工作区中，手动触发这些管道。

步骤 6：使用 CI/CD 部署项目和管道

若要了解如何将 Azure Synapse 工作区与 Azure DevOps 或 GitHub 集成，以及如何将项目部署到目标区域工作区，请按照 Azure Synapse 工作区的持续集成和持续交付 (CI/CD) 中的步骤操作。

将工作区与 Azure DevOps 集成后，你会发现一个名为 workspace_publish 的分支。 此分支包含工作区模板，模板中包括笔记本、SQL 脚本、数据集、链接服务、管道、触发器和 Spark 作业定义等项目的定义。

这个来自 Azure DevOps 存储库的屏幕截图显示了项目和其他组件的工作区模板文件。



显示 workspacepublish 的屏幕截图。

可以使用工作区模板通过 Azure DevOps 发布管道将项目和管道部署到工作区。

如果工作区未与 GitHub 或 Azure DevOps 集成，则必须手动重新创建或编写自定义 PowerShell 或 Azure CLI 脚本，以将所有项目、管道、链接服务、凭据、触发器和 Spark 定义部署到目标区域工作区。

备注

此过程要求你不断更新管道和代码项目，以包含对源区域工作区中的 Spark 和无服务器 SQL 池、对象和角色所做的任何更改。

步骤 7：创建共享集成运行时

若要创建 SHIR，请按照创建和配置自承载集成运行时中的步骤操作。

步骤 8：向托管标识分配 Azure 角色

为默认附加 Data Lake Storage Gen2 帐户上的新工作区的托管标识分配 Storage Blob Contributor 访问权限。 同时在使用 SA-MI 进行身份验证的其他存储帐户上分配访问权限。 为所有必需的存储帐户的 Microsoft Entra 用户和组分配 Storage Blob Contributor 或 Storage Blob Reader 访问权限。

Azure 门户

按照向工作区托管标识授予权限中的步骤将“存储 Blob 数据参与者”角色分配给工作区的托管标识。

Azure PowerShell

将“存储 Blob 数据参与者”角色分配给工作区的托管标识。

将存储 Blob 数据参与者添加到存储帐户上的工作区托管标识。 执行 New-AzRoleAssignment 时会出现错误，错误消息为“Exception of type 'Microsoft.Rest.Azure.CloudException' was thrown.”，但它会在存储帐户上创建所需的权限。

PowerShell

```
$workSpaceIdentityObjectID= (Get-AzSynapseWorkspace -ResourceGroupName $resourceGroupName -Name $workspaceName).Identity.PrincipalId
$scope = "/subscriptions/$($subscriptionId)/resourceGroups/$($resourceGroupName)/providers/Microsoft.Storage/storageAccounts/$($storageAccountName)"

$roleAssignedforManagedIdentity=New-AzRoleAssignment -ObjectId $workSpaceIdentityObjectID `
  -RoleDefinitionName "Storage Blob Data Contributor" `
  -Scope $scope -ErrorAction SilentlyContinue
```

Azure CLI

获取工作区托管标识的角色名称、资源 ID 和主体 ID，然后将存储 Blob 数据参与者 Azure 角色添加到 SA-MI。

Azure CLI

```
# Getting Role name
$roleName =az role definition list --query "[?contains(roleName, 'Storage Blob Data Contributor')].{roleName:roleName}" --output tsv

#Getting resource id for storage account
$scope= (az storage account show --name $storageAccountName|ConvertFrom-Json).id

#Getting principal ID for workspace managed identity
$workSpaceIdentityObjectID=(az synapse workspace show --name $workspaceName --resource-group $resourceGroupName|ConvertFrom-Json).Identity.PrincipalId
# Adding Storage Blob Data Contributor Azure role to SA-MI
az role assignment create --assignee $workSpaceIdentityObjectID `
--role $roleName `
--scope $scope
```

步骤 9：分配 Azure Synapse RBAC 角色

为所有需要访问目标工作区的用户添加单独的角色和权限。 以下 PowerShell 和 CLI 脚本可将 Microsoft Entra 用户添加为目标区域工作区中的 Synapse 管理员角色。

若要获取所有 Azure Synapse RBAC 角色名称，请参阅 Azure Synapse RBAC 角色。

Synapse Studio

若要在 Synapse Studio 中添加或删除 Azure Synapse RBAC 分配，请按照如何在 Synapse Studio 中管理 Azure Synapse RBAC 角色分配中的步骤操作。

Azure PowerShell

以下 PowerShell 脚本可将 Synapse 管理员角色分配添加到 Microsoft Entra 用户或组。 你可以在以下命令中使用 -RoleDefinitionId 来取代 -RoleDefinitionName，以将用户添加到工作区：

PowerShell

```
New-AzSynapseRoleAssignment `
 -WorkspaceName $workspaceName `
 -RoleDefinitionName "Synapse Administrator" `
 -ObjectId 1c02d2a6-ed3d-46ec-b578-6f36da5819c6
```

```
Get-AzSynapseRoleAssignment -WorkspaceName $workspaceName
```

若要获取源区域工作区中的 ObjectId 和 RoleId，请运行 Get-AzSynapseRoleAssignment 命令。 将相同的 Azure Synapse RBAC 角色分配给目标区域工作区中的 Microsoft Entra 用户或组。

你还可以使用 -SignInName 作为参数来取代 -ObjectId，并在其中提供用户的电子邮件地址或用户主体名称。 若要详细了解可用的选项，请参阅 Azure Synapse RBAC - PowerShell cmdlet。

Azure CLI

获取用户的对象 ID，并将所需的 Azure Synapse RBAC 权限分配给 Microsoft Entra 用户。 可以为 --assignee 参数提供用户的电子邮件地址 (username@contoso.com)。

Azure CLI

```
az synapse role assignment create `
--workspace-name $workspaceName `
--role "Synapse Administrator" --assignee adasdasdd42-0000-000-xxx-xxxxxxx
```

```
az synapse role assignment create `
--workspace-name $workspaceName `
--role "Synapse Contributor" --assignee "user1@contoso.com"
```

若要详细了解可用的选项，请参阅 Azure Synapse RBAC - CLI。

步骤 10：上传工作区包

将所有必需的工作区包上传到新工作区。 若要自动执行上传工作区包的过程，请参阅 Microsoft Azure Synapse Analytics Artifacts 客户端库。

步骤 11：权限

若要为目标区域 Azure Synapse 工作区设置访问控制，请按照如何为 Azure Synapse 工作区设置访问控制中的步骤操作。

步骤 12：创建托管专用终结点

若要在目标区域工作区中重新创建源区域工作区中的托管专用终结点，请参阅创建数据源的托管专用终结点。

弃用

如果你要放弃目标区域工作区，请删除目标区域工作区。 为此，请从门户中的仪表板转到资源组，选择该工作区，然后选择“资源组”页顶部的“删除”。

清理

若要提交更改并完成工作区移动，请在测试目标区域中的工作区后删除源区域工作区。 为此，请从门户中的仪表板转到具有源区域工作区的资源组，选择该工作区，然后选择“资源组”页顶部的“删除”。

有关更多信息： * 详细了解 Azure Synapse Analytics。 * 详细了解 Azure Synapse Analytics 常见问题解答。 * 详细了解 有关将数据加载到 Azure Synapse Analytics 中的专用 SQL 池的最佳做法。 * 详细了解 备份和还原 Azure Synapse Analytics 中的专用 SQL 池。 * 详细了解 Azure Synapse 托管虚拟网络。 * 详细了解 Azure Synapse 托管专用终结点。

如有任何问题，请联系您的 Azure 支持团队。

HDInsight

目前并不支持将 HDIsight 从一个区域迁移到另一个区域。我们建议您在新区域中创建和配置 HDInsight。

先决条件

- 确认 Azure 订阅允许在目标区域中创建 HDInsight 及其对应资源。
- 先了解 HDInsight 所需的所有服务再规划迁移策略。必须对于迁移涉及的服务选择适当的迁移策略。

元数据迁移

备份和还原

涉及到 HDInsight 元数据，如果存储在 Azure SQL 的元数据 DB 中，可以使用 Azure SQL 数据库的备份和还原，请参阅使用自动数据库备份在 Azure SQL 数据库中恢复数据库。

在目标源数据库中，相应的字段表格中，将源数据存储地址修改为新数据存储地址。

元数据脚本迁移

使用脚本迁移 Hive 元存储：

1. 从本地 Hive 元存储生成 Hive DDL。可以考虑使用包装器 bash 脚本完成此步骤。
2. 编辑生成的 DDL，将源数据存储地址修改为新数据存储地址。
3. 针对 HDInsight 群集中的元存储运行更新的 DDL。
4. 确保源和目标之间的 Hive 元存储版本兼容。

迁移

验证一切都按预期工作后，请为迁移安排停机时间。在此停机期间，请执行以下操作：

1. 备份所有存储在本地群集节点上的暂时性数据。
2. 停止 HDInsight 群集。
3. 使用 AzCopy 或类似工具将 Azure 存储帐户中的数据迁移到新区域。
4. 在目标 Azure 区域中创建新的 HDInsight 资源，请参阅了解如何创建基于 Linux 的 HDInsight 群集。将迁移的存储资源作为主要连接存储附加。
5. 导入任何已备份的暂时性数据。
6. 通过 ddl 语句重建对象。
7. 使用新群集启动作业/继续处理。

特定于工作负载的指南

以下文档提供有关如何迁移特定工作负载的指南：

- 迁移 HBase
- 迁移 Kafka
- 迁移 Hive/Interactive Query

验证

执行验证测试，以确保作业在新群集上按预期工作。

有关更多信息

- 查阅 Azure HDInsight 文档。
- 通过完成 HDInsight 教程来刷新您的知识。
- 有关缩放 HDInsight 群集的帮助，请参阅使用 PowerShell 管理 HDInsight。
- 了解如何使用 AzCopy。

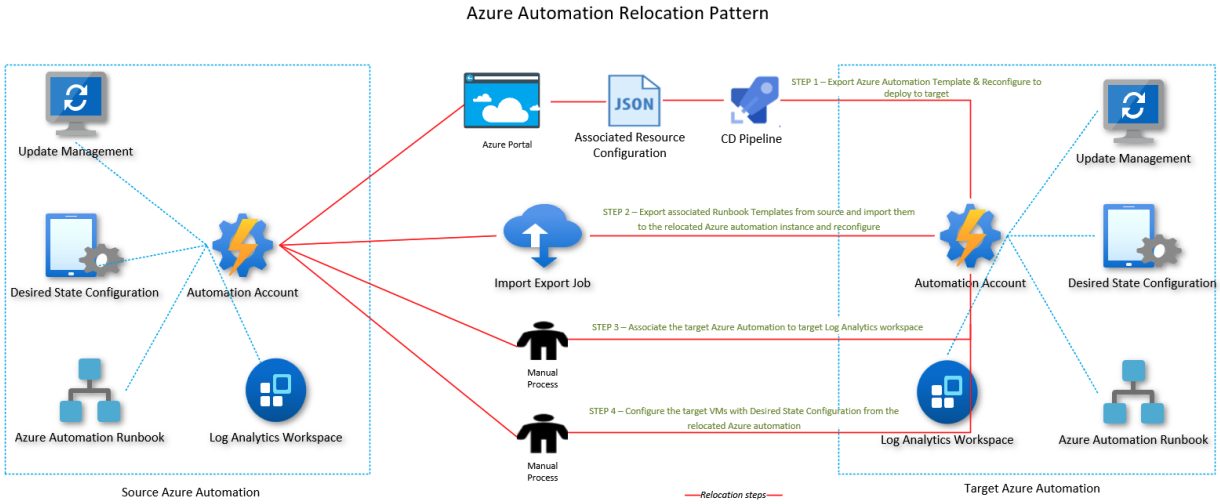
迁移 Azure 自动化

概述

Azure 自动化提供基于云的自动化、操作系统更新和配置服务，用于支持 Azure 环境和非 Azure 环境之间的一致管理。 Azure 自动化包括流程自动化、配置管理、更新管理、共享功能和异类功能。

Azure 自动化不能直接从一个区域移至另一个区域。 一种解决方法是在旧的区域"导出模板"后，新区域修改参数后重新创建 Azure 自动化，然后将移动的资源与新实例关联。 在新的 Azure 自动化在新区域中运行后，就可以删除之前区域中的旧自动化。

在下图中，红色流线演示了目标实例的重新部署以及配置移动。更多信息请阅读 将 Azure 自动化迁移到另一个区域。



Azure Automation Relocation Pattern

相关参考文档

- Azure 自动化文档

迁移 Azure Monitor

目录

- 概述
- Log Analytics 工作区
  - 先决条件
  - 停机时间
  - 迁移步骤
- Application Insights
  - 可用性测试
- 工作簿
- 操作组
- 总结

概述

Azure 监控器（Monitor）本身没有区域属性，不需要进行迁移。
但 Azure 监控器中所包含的一些功能可能是具有区域性的，比如 Log Analytics 工作区、Application Insights、可用性测试、工作簿 等。
不同的功能所支持的区域可能会略有不同，并且可能会随着产品的迭代升级而发生变化。
在迁移规划阶段就应该尽早确认功能在目标区域是否支持，并作出合理规划。

Log Analytics 工作区

Log Analytics 工作区的迁移计划必须包括使用 Log Analytics 工作区记录数据的任何资源的迁移。
Log Analytics 工作区本身不支持将工作区数据从一个区域迁移到另一区域和关联设备。 相反，必须在目标区域中新建 Log Analytics 工作区，并在新工作区中重新配置设备和设置。

先决条件

- 若要将工作区配置导出到某个可部署到另一个区域的模板，你需要具有 Log Analytics 参与者 或 监视参与者角色或权限更高的角色。
- 查明当前关联到你的工作区的所有资源，包括：连接的代理、诊断设置、已安装的解决方案、数据收集器 API、链接服务、警报、查询包。 （参考）
- 验证你的 Azure 订阅是否允许在目标区域中创建 Log Analytics 工作区。

停机时间

要了解可能涉及的故障时间，请参阅 面向 Azure 的云采用框架：选择重定位方法。

迁移步骤

您需要先将 源 Log Analytics 工作区的模板导出，修改调整后，在新目标区域进行重新部署。
详细迁移步骤请参考 将 Azure Monitor - Log Analytics 工作区重新定位到另一个区域。

Application Insights

在区域之间传输现有的 Application Insights 资源是不受支持的，并且你无法将历史数据迁移到新区域。
关于具体的解决方法，您可以参考 如何将 Application Insights 资源移动到新区域 中的内容。

可用性测试

可用性测试功能依赖于基于工作区的 Application Insights 资源，但可用性测试的执行区域与所属 Application Insights 资源所在区域无关。
您可以在 Application Insights 资源的可用性窗格中，创建或编辑不同区域的可用性测试。
详细内容，请参阅 Application Insights 可用性测试。

工作簿

如果想要将 Azure 工作簿资源移动到其他 Azure 区域，可以参考 将 Azure 工作簿移动到另一个区域 中的内容。

操作组

你无需将操作组（Action Group）迁移到其他区域，平台将自动确保其可用性。请放心，北部 1 区/东部 1 区的退役不会影响操作组的正常运行。

总结

在生产环境迁移前，请先在测试环境进行测试验证。

如果遇到任何问题，可以参考 Azure 官方文档或联系 Azure 技术支持。

有关更多信息：

- Azure Monitor
- Log Analytics 工作区概述

- Application Insights 概述

迁移 Azure Site Recovery

概述

您无法跨 Azure 区域移动现有的 Azure 站点恢复(ASR)设置。

Azure Site Recovery 本身用于源区域 Region1 的 VM 到目标区域 Region2 的恢复，需要将 Azure Recovery Vault 创建在目标区域 Region2。
当你决定迁移 Azure Site Recovery 区域，相当于更改 VM 恢复的目标区域，因此目标区域以前存在的配置无法重复使用。

您可以 禁用 现有配置并在目标 Azure 区域中设置新的站点恢复解决方案。
详细内容请参考 将 Azure Recovery Vault 和 Site Recovery 重新安置到其他区域。

总结

在生产环境迁移前，请先在测试环境进行测试验证。
如果遇到任何问题，可以参考 Azure 官方文档或联系 Azure 技术支持。

有关更多信息：

* Azure 到 Azure 的灾难恢复
* Vmware 到 Azure 的灾难恢复
* Hyper-V 到 Azure 的灾难恢复
* 物理机 到 Azure 的灾难恢复

迁移 Azure Backup

概述

Azure 备份是基于 Azure 的服务，用于备份（或保护）和还原 Azure 中的数据。
该服务可以保护本机 Azure 资源（如 VM）以及来自混合环境的非 Azure 资源（包括在本地服务器上运行的工作负载）。
所有备份都存储在 Azure 的恢复服务保管库中。
Azure 备份不支持将备份数据从一个恢复服务保管库重定位到另一个恢复服务保管库。
若要继续保护资源，必须将其注册并备份到新区域中的恢复服务保管库。

先决条件

- 复制 Azure Resource Vault 的内部资源或设置。
  - 网络防火墙重新配置
  - 警报通知。
  - 移动工作簿（如果已配置）
  - 诊断设置重新配置
- 列出所有恢复服务保管库依赖项资源。 最常见的依赖项包括：
  - Azure 虚拟机 (VM)
  - 公共 IP 地址
  - Azure 虚拟网络
  - Azure 恢复服务保管库
- 不管 VM 是否连同保管库一起移动，都始终可以从保管库中保留的备份历史记录还原该 VM。
- 复制备份 VM 配置元数据，以便在重定位完成后进行验证。
- 确认源资源保管库使用的所有服务和功能在目标区域中受支持。

迁移

如果客户需要在 Azure 区域之间迁移，则应首先在目标区域中创建可以保护新区域中资源的新恢复服务保管库。
要迁移受 Azure 备份保护的 Azure 资源，则首先需要对受保护的资源 停止保护并保留备份数据。
然后，可以将资源迁移到目标区域，并且可以在新创建的恢复保管库中启用保护。
对于非 Azure 资源，客户将遵循相同的过程，但不需要迁移资源。

有关迁移 Azure 备份的详细内容，可参阅 将 Azure 备份重定位到另一个区域。

总结

在生产环境迁移前，请先在测试环境进行测试验证。

如果遇到任何问题，可以参考 Azure 官方文档或联系 Azure 技术支持。

有关更多信息：

* 通过完成 备份教程来刷新您的知识。

* 查阅 Azure 备份概述。

迁移 Azure Event Hubs

目录

- 简介
- 先决条件
- 服务终结点注意事项
- 专用终结点注意事项
- 迁移命名空间
- 迁移专用群集

简介

本手册旨在指导您如何将 Azure Event Hubs 从一个区域迁移到另一个区域。

您无法跨 Azure 区域直接迁移 Azure 事件中心资源。事件中心服务没有数据导出或导入功能。您可以将事件中心资源导出为资源管理器模板，然后针对目标 Azure 区域调整导出的模板并重新创建资源。

先决条件

- 确保帐户使用的服务和功能在目标区域中受支持。
- 如果在命名空间中为事件中心启用了捕获功能，请在移动事件中心命名空间之前首先移动 Azure 存储或 Azure Data Lake Store Gen 2 帐户。 还可以按照与本文所述步骤类似的步骤，将包含存储和事件中心命名空间的资源组移到另一个区域。
- 如果事件中心命名空间位于事件中心群集中，则在执行本文中的步骤之前，请将专用群集移到目标区域。 还可以使用 GitHub 上的快速入门模板创建事件中心群集。 在模板中，删除 JSON 的命名空间部分以仅创建群集。
- 标识所有资源依赖项。 根据事件中心的部署方式，以下服务可能需要在目标区域中部署：
    - 公共 IP
    - 虚拟网络
    - 事件中心命名空间
    - 事件中心群集
    - 存储帐户

提示

启用捕获功能后，可以迁移源区域中的存储帐户，也可以使用目标区域中的现有存储帐户。

- 标识所有依赖资源。 事件中心是一个消息传递系统，允许应用程序发布和订阅消息。 考虑目标区域的应用程序是否需要它在源区域上具有的同一组依赖服务的消息传递支持。

服务终结点注意事项

通过 Azure 事件中心的虚拟网络服务终结点可将访问限制为指定虚拟网络。 此外，还可通过这些终结点将访问限制为一系列 IPv4（Internet 协议版本 4）地址范围。 任何从外部连接到事件中心的用户都无法访问这些资源。 如果在事件中心资源的源区域中配置了服务终结点，则需要在目标区域中执行相同的操作。

若要成功将事件中心重新创建到目标区域，必须事先创建 VNet 和子网。 如果使用 Azure 资源转移器工具执行所有这些资源的移动，则不会自动配置服务终结点。 因此，需要手动配置服务终结点，这可以通过 Azure 门户、Azure CLI 或 Azure PowerShell 来完成。

专用终结点注意事项

Azure 专用链接提供从虚拟网络到 Azure 平台即服务 (PaaS)、客户拥有的服务或 Microsoft 合作伙伴服务的专用连接。 专用链接简化了网络体系结构，并通过消除数据在公共 Internet 上的暴露来保护 Azure 中终结点之间的连接。

若要成功在目标区域中重新创建事件中心，必须事先创建 VNet 和子网，然后才能进行实际重新创建。

迁移命名空间

要迁移命名空间到另外一个区域，请参考官方文档说明：将 Azure 事件中心命名空间移到另一个区域

迁移专用群集

要迁移专用群集到另外一个区域，请参考官方文档说明：将 Azure 事件中心专用群集移到另一个区域

迁移 Azure Event Grid

目录

- 简介
- 事件网格域的迁移
- 事件网格系统主题的迁移
- 事件网格自定义主题的迁移

简介

本文介绍将 Azure 事件网格域重定位到另一个区域的建议方法、指南和做法。

出于多种原因，你可能希望将现有 Azure 资源从一个区域移到另一个区域。 你可以采取以下建议：

- 利用新的 Azure 区域。
- 部署仅在特定区域可用的功能和服务。
- 满足内部策略和治理要求。
- 与公司合并和收购保持一致
- 满足容量计划要求。

针对 Azure Event Grid 的迁移，分作 3 种不同的迁移场景： - 事件网格域的迁移 - 事件网格系统主题的迁移 - 事件网格自定义主题的迁移

事件网格域的迁移

大致步骤如下：

- 将域资源导出到 Azure 资源管理器模板。

> **重要**
> 域资源和域中的主题会导出到该模板。 对域主题的订阅不会导出。

- 使用该模板将域部署到目标区域。
- 在目标区域中手动创建对域主题的订阅。 在当前区域中将域导出到模板时，对域主题的订阅不会导出。 因此，请在目标区域中创建域和域主题后创建这些订阅。
- **验证部署。** 将一个事件发送到该域中的某个域主题，并验证是否会调用与该订阅关联的事件处理程序。
- 若要**完成移动**，请从源区域中删除域。

详细步骤请查看：事件网格域的迁移的详细步骤

事件网格系统主题的迁移

大致步骤如下：

- 将包含 Azure 存储帐户及其关联的系统主题的资源组导出到资源管理器模板。 你还可以仅导出系统主题的模板。 如果走此路线，请记得在移动系统主题之前将 Azure 事件源（在此示例中为 Azure 存储帐户）移动到另一个区域。 然后，在系统主题的已导出模板中，更新目标区域中的存储帐户的外部 ID。
- **修改模板**来添加 endpointUrl 属性，使之指向订阅系统主题的 Webhook。 导出系统主题时，其订阅（在本例中为 Webhook）也将导出到模板，但 endpointUrl 属性不包括在内。 因此，你需要将其更新为指向订阅该主题的终结点。 另外，还要更新 location 属性的值，使之指向新位置或区域。 对于其他类型的事件处理程序，你只需更新位置。
- **使用模板**将资源部署到目标区域。 你需要指定要在目标区域中创建的存储帐户和系统主题的名称。
- **验证部署**。 验证将文件上传到目标区域中的 blob 存储时是否调用 Webhook。
- 若要**完成移动**，请从源区域中删除资源（事件源和系统主题）。

详细步骤请查看：事件网格系统主题的迁移的详细步骤

事件网格自定义主题的迁移

大致步骤如下：

- 将自定义主题资源导出到 Azure 资源管理器模板。
- **修改模板**来添加 endpointUrl 属性，使之指向订阅自定义主题的 Webhook。 导出自定义主题时，其订阅（在本例中为 Webhook）也将导出到模板，但 endpointUrl 属性不包括在内。 因此，你需要将其更新为指向订阅该主题的终结点。 另外，还要更新 location 属性的值，使之指向新位置或区域。 对于其他类型的事件处理程序，你只需更新位置。
- **使用模板**将资源部署到目标区域。 你需要指定要在目标区域中创建的自定义主题的名称。
- **验证部署**。 验证目标区域中是否已创建自定义主题。
- 若要**完成移动**，请从源区域中删除自定义主题。

详细步骤请查看：事件网格自定义主题的迁移的详细步骤

迁移事件网格域

目录

- 先决条件
- 准备
- 重新部署
- 丢弃或清理

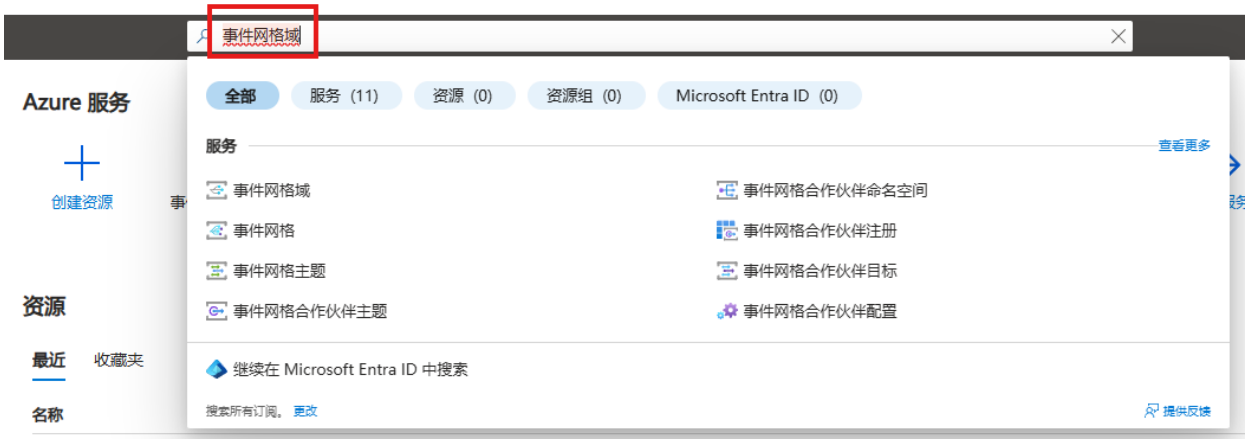
先决条件

- 请确保在目标区域中可以使用事件网格服务。

准备

若要开始操作，请导出用于该事件网格域的资源管理器模板。

1. 登录到 Azure 门户。
2. 在搜索栏中，键入“事件网格域”，然后从结果列表中选择“事件网格域”。

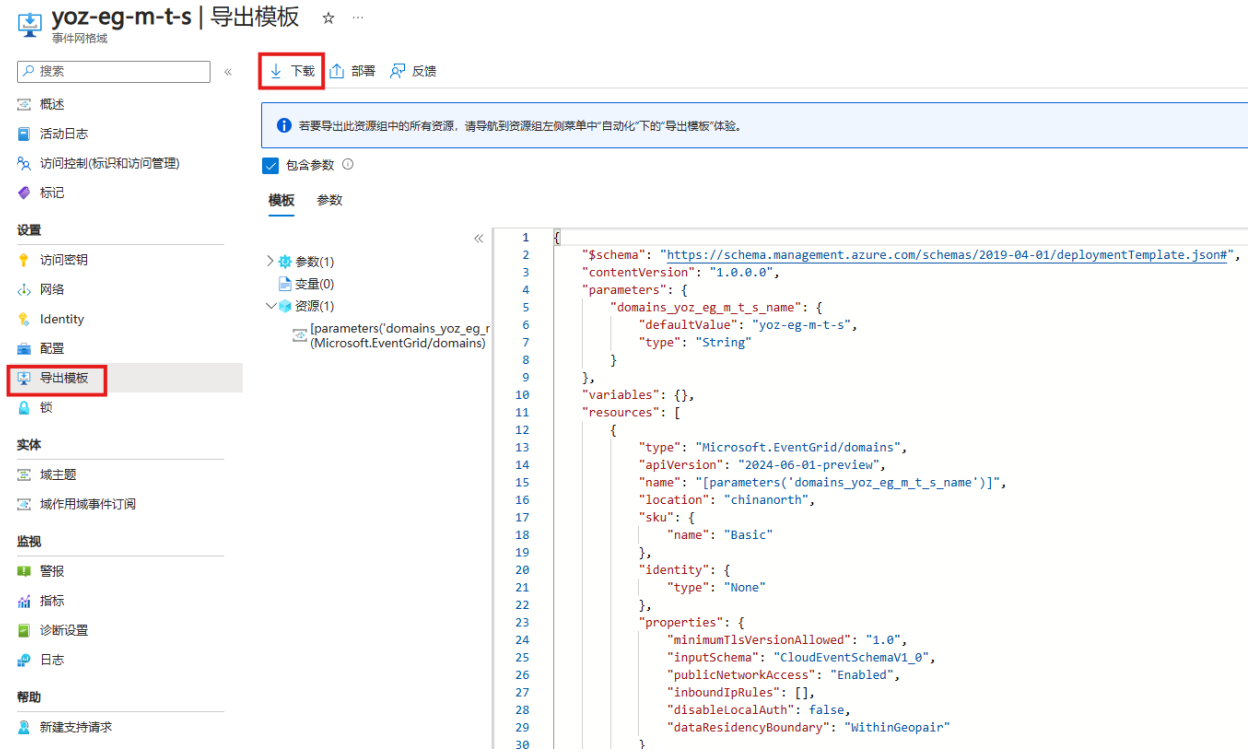


搜索并选择 Azure 事件网格域的屏幕截图

3. 选择要导出到资源管理器模板的域。

选择域页的屏幕截图

4. 在“事件网格域”页上，选择左侧菜单中“设置”下的“导出模板”，然后选择工具栏上的“下载”。



导出模板 ->“下载”页的屏幕截图

重要

域和域主题会导出。 对域主题的订阅不会导出。 因此，需要在移动域主题之后为域主题创建订阅。

5. 找到从门户下载的 .zip 文件，并将该文件解压缩到所选的文件夹。 此 zip 文件包含模板和参数 JSON 文件。

6. 在你选择的编辑器中打开 template.json。

7. 将域资源的 location 更新为目标区域或位置。 区域的代码是不带空格的区域名称，例如 China North 3 等同于 chinanorth3。

```
"type": "Microsoft.EventGrid/domains",
"apiVersion": "2020-06-01",
```

```
"name": "[parameters('domains_yoz_eg_m_t_s_name')]",
"location": "chinanorth3。",
```

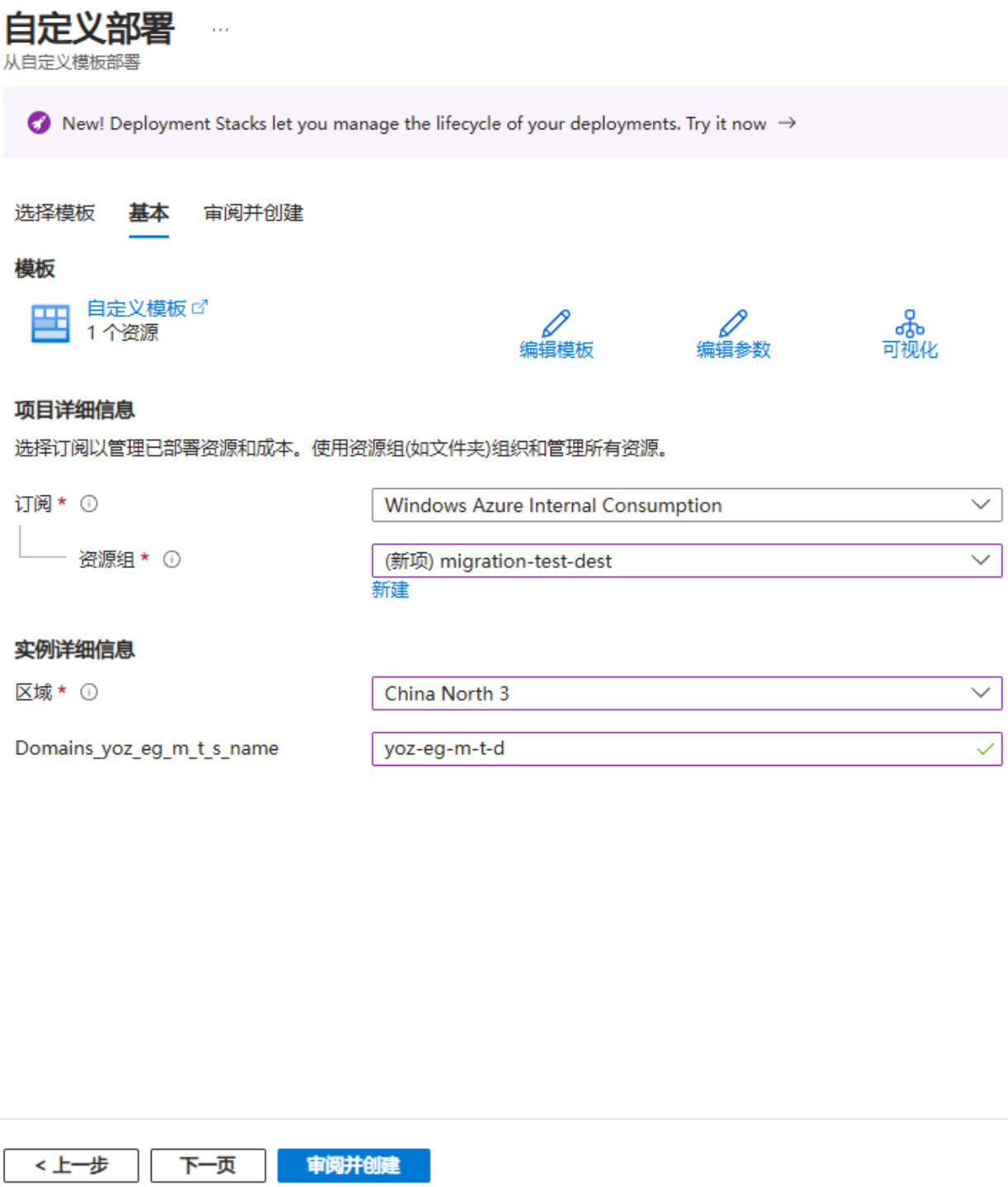
8. 保存该模板。

重新部署

在目标区域中部署该模板以创建域和域主题。

1. 在 Azure 门户中，选择“创建资源”。
2. 在“搜索市场”中键入“模板部署”，然后按 ENTER。
3. 选择“模板部署”。
4. 选择“创建” 。
5. 选择“在编辑器中生成自己的模板”。
6. 选择“加载文件”，然后按说明加载在上一部分下载的 template.json 文件。
7. 选择“保存”以保存该模板。
8. 在“自定义部署”页上执行以下步骤：
    1. 选择 Azure 订阅。
    2. 选择目标区域中现有的资源组，或者创建一个资源组。
    3. 对于“区域”，请选择目标区域。 如果选择了现有资源组，则此设置为只读。
    4. 对于“域名”，请为该域输入新名称。

5. 选择“审阅并创建”。



6. 模板的验证成功之后，请选择页面底部的“创建”来部署资源。
7. 部署成功后，请选择“转到资源组”，以导航到资源组页。 确认资源组中存在某个域。 选择该域。 确认该域中存在域主题。

丢弃或清理

若要完成移动，请删除源区域中的域。

如果需要重新开始，请删除目标区域中的域，并重复本文的准备和重新创建部分中的步骤。

若要通过使用 Azure 门户来删除域，请执行以下步骤：

1. 在 Azure 门户顶部的搜索窗口中，键入“事件网格域”，然后从搜索结果中选择“事件网格域”。
2. 选择要删除的域，然后从工具栏中选择“删除”。
3. 在确认页上，输入资源的名称，然后选择“删除”。

若要通过使用 Azure 门户删除包含域的资源组，请执行以下步骤：

1. 在 Azure 门户顶部的搜索窗口中，键入“资源组”，然后从搜索结果中选择“资源组” 。
2. 选择要删除的资源组，然后从工具栏中选择“删除”。
3. 在确认页上，输入资源组的名称，然后选择“删除”。

迁移事件网格系统主题

目录

- 先决条件
- 准备
- 重新部署
- 验证
- 丢弃或清理

先决条件

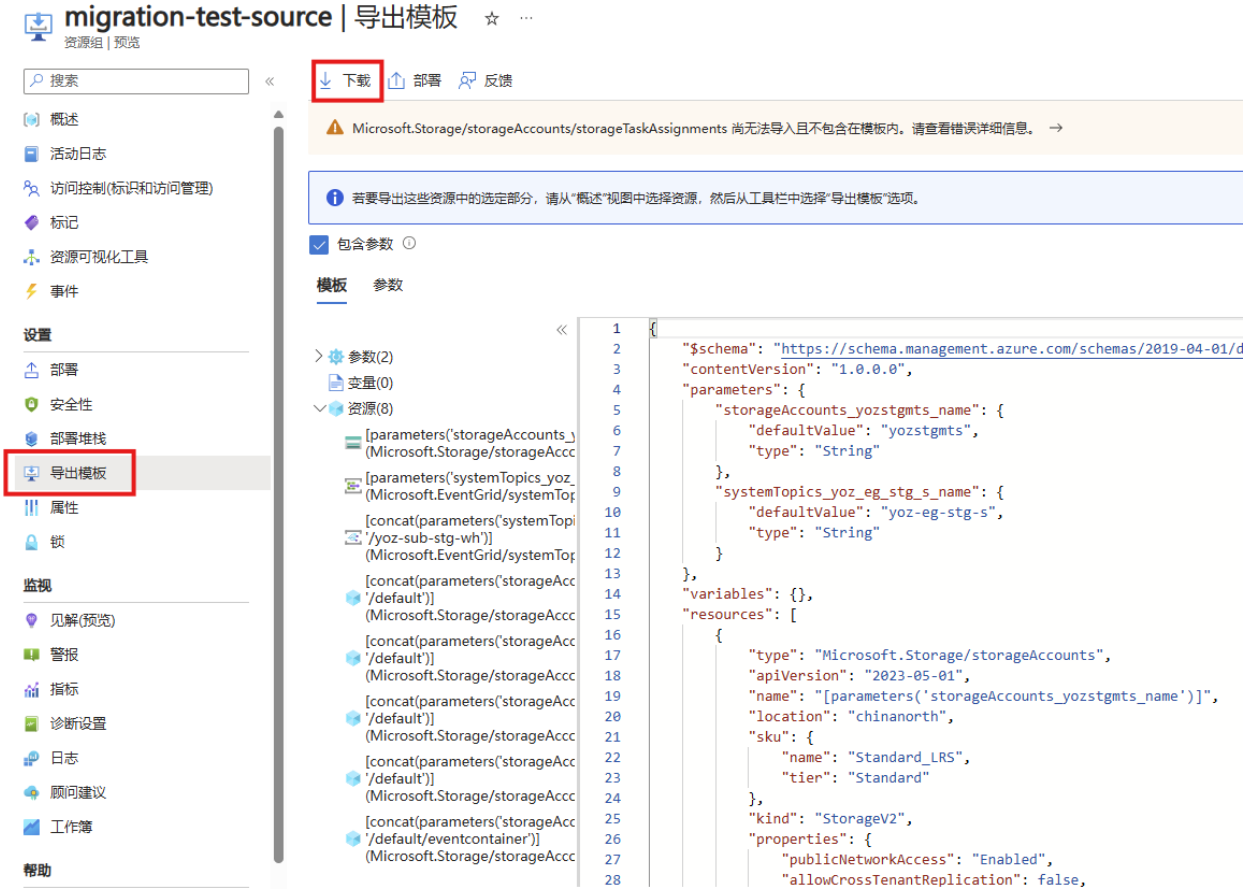
- 完成快速入门：使用 Azure 事件网格将 Blob 存储事件路由到 Web 终结点（Azure 门户）。 此步骤是可选的。 可以执行此步骤来测试本文中的步骤。 在与应用服务和应用服务计划不同的资源组中保留存储帐户。
- 请确保在目标区域中可以使用事件网格服务。

准备

若要开始，请为包含系统事件源（Azure 存储帐户）及其关联的系统主题的资源组导出资源管理器模板。

1. 登录到 Azure 门户。
2. 在左侧菜单中选择“资源组”。 然后，选择为其创建了系统主题的事件源所在的资源组。 在以下示例中，它是 Azure 存储帐户。 资源组包含存储帐户及其关联的系统主题。

3. 在左侧菜单中的“设置”下选择“导出模板”，然后在工具栏上选择“下载”。



4. 找到从门户下载的 .zip 文件，并将该文件解压缩到所选的文件夹。 此 zip 文件包含模板和参数 JSON 文件。

5. 在所选编辑器中打开 template.json。

6. Webhook 的 URL 未导出到模板。 因此，请执行以下步骤：

    1. 在模板文件中，搜索“WebHook”。

    2. 在“属性”部分的最后一行的末尾添加一个逗号 (,) 字符。 在此示例中，它是 “preferredBatchSizeInKilobytes”: 64。

    3. 添加 endpointUrl 属性并将值设置为你的 Webhook URL，如以下示例所示。

```
"destination": {
    "properties": {
        "maxEventsPerBatch": 1,
        "preferredBatchSizeInKilobytes": 64,
        "endpointUrl": "https://spegridsite.chinacloudsites.cn/api/updates"
    },
    "endpointType": "WebHook"
}
```

> **备注**
>
> 对于其他类型的事件处理程序，所有属性都会导出到模板。 你只需将 location 属性更新为目标区域，如下一步所示。

7. 将存储帐户资源的 location 更新为目标区域或位置。 区域的代码是不带空格的区域名称，例如 China North 3 等同于 chinanorth3。

```
"type": "Microsoft.Storage/storageAccounts",
"apiVersion": "2019-06-01",
"name": "[parameters('storageAccounts_yozstgmts_name')]",
"location": "chinanorth3",
```

8. 重复此步骤以更新模板中系统主题资源的 location。

```
"type": "Microsoft.EventGrid/systemTopics",
"apiVersion": "2020-04-01-preview",
"name": "[parameters('systemTopics_yoz_eg_stg_s_name')]",
"location": "chinanorth3",
```

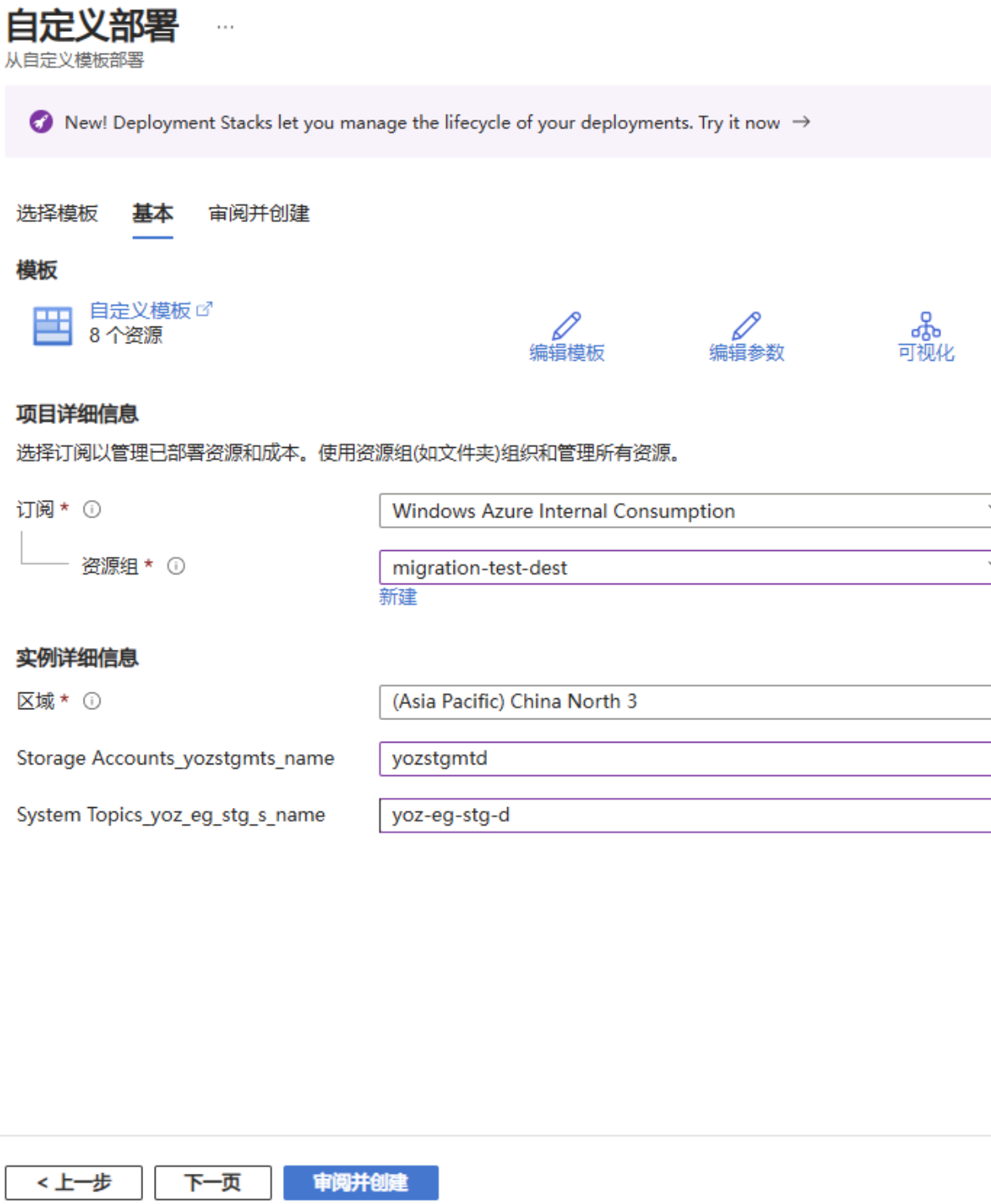
9. 保存该模板。

重新部署

部署模板，在目标区域中为存储帐户创建一个存储帐户和系统主题。

1. 在 Azure 门户中，选择“创建资源”。
2. 在“搜索市场”中键入“模板部署”，然后按 ENTER。
3. 选择“模板部署”。
4. 选择“创建”。
5. 选择“在编辑器中生成自己的模板”。
6. 选择“加载文件”，然后按说明加载在上一部分下载的 template.json 文件。
7. 选择“保存”以保存该模板。
8. 在“自定义部署”页上执行以下步骤。
    1. 选择 Azure 订阅。
    2. 选择目标区域中现有的资源组，或者创建一个资源组。
    3. 对于“区域”，请选择目标区域。 如果选择了现有资源组，则此设置为只读。
    4. 对于“系统主题名称”，请输入将与存储帐户关联的系统主题的名称。

5. 对于“存储帐户名称”，请输入要在目标区域中创建的存储帐户的名称。



6. 在页面底部选择“审阅并创建”。
7. 在“审阅并创建”页上查看基本信息，然后选择“创建”。

验证

1. 部署成功后，选择“转到资源组”。
2. 在“资源组”页面上，验证是否已创建事件源（在本例中为 Azure 存储帐户）和系统主题。

3. 将文件上传到 Azure Blob 存储中的容器，并验证 Webhook 是否已收到该事件。 有关详细信息，请参阅将事件发送到终结点。

丢弃或清理

若要完成移动，请在源区域中删除包含存储帐户及其关联的系统主题的资源组。

如果需要重新开始，请在目标区域中删除资源组，然后重复本文的准备和重新创建部分中的步骤。

若要使用 Azure 门户删除资源组（源或目标），请执行以下操作：

1. 在 Azure 门户顶部的搜索窗口中，键入“资源组”，然后从搜索结果中选择“资源组”。
2. 选择要删除的资源组，然后从工具栏中选择“删除资源组”。
3. 在确认页上，输入资源组的名称，然后选择“删除”。

迁移事件网格自定义主题

目录

- 先决条件
- 准备
- 重新部署
- 验证

先决条件

- 完成快速入门：使用 Azure 门户和 Azure 事件网格将自定义事件路由到 Web 终结点。 请执行此步骤，以便可以测试本文中的步骤。
- 请确保在目标区域中可以使用事件网格服务。 参阅各区域的产品可用性。

准备

若要开始操作，请导出用于该自定义主题的资源管理器模板。

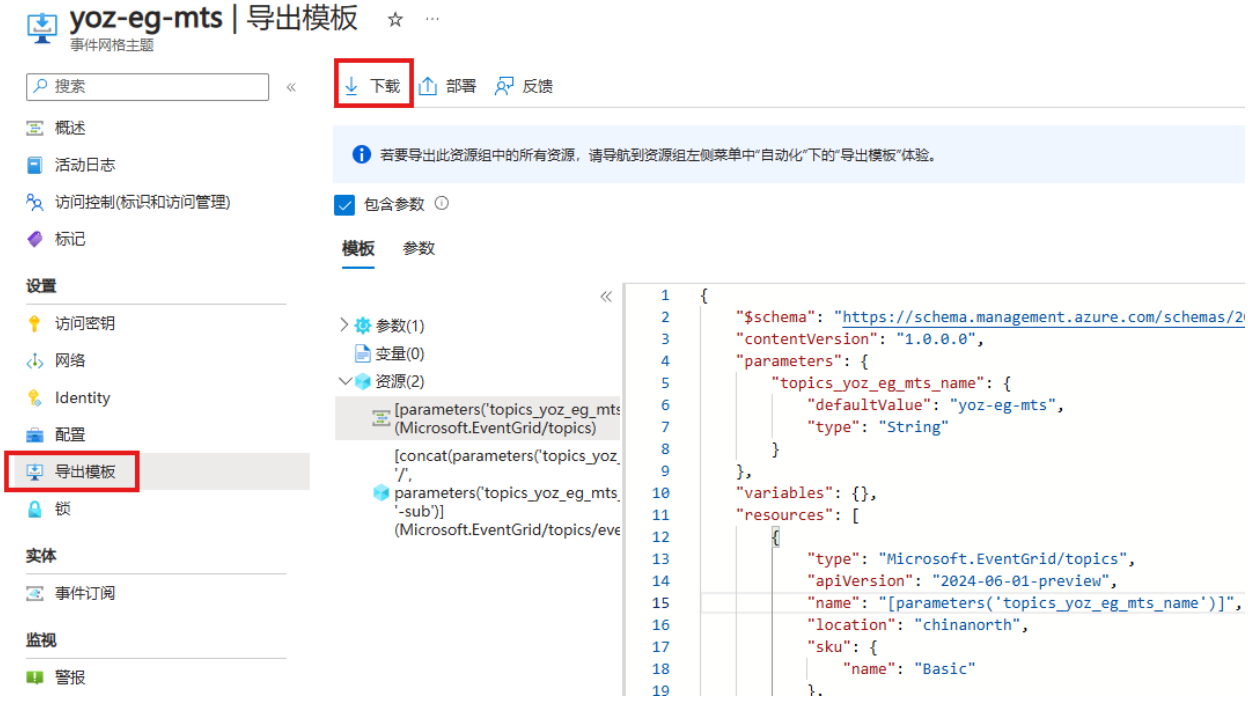
1. 登录到 Azure 门户。
2. 在搜索栏中，键入“事件网格主题”，然后从结果列表中选择“事件网格主题”。

搜索并选择 Azure 事件网格主题页面的屏幕截图

3. 选择要导出到资源管理器模板的主题。

选择自定义主题页面的屏幕截图

4. 在“事件网格主题”页上，选择左侧菜单中“设置”下的“导出模板”，然后选择工具栏上的“下载”。



导出模板 ->“下载”页的屏幕截图

5. 找到从门户下载的 .zip 文件，并将该文件解压缩到你选择的某个文件夹中。 此 zip 文件包含模板和参数 JSON 文件。

6. 在你选择的编辑器中打开 template.json。

7. Webhook 的 URL 未导出到模板。 因此，请执行以下步骤：

    1. 在模板文件中，搜索“WebHook”。

    2. 在“属性”部分的最后一行的末尾添加一个逗号 (,) 字符。 在此示例中，它是 “preferredBatchSizeInKilobytes”: 64。

    3. 添加 endpointUrl 属性并将值设置为你的 Webhook URL，如以下示例所示。

```
"destination": {
    "properties": {
        "maxEventsPerBatch": 1,
        "preferredBatchSizeInKilobytes": 64,
        "endpointUrl": "https://spegridsite.chinacloudsites.cn/api/updates"
    },
    "endpointType": "WebHook"
}
```

> **备注**
>
> 对于其他类型的事件处理程序，所有属性都会导出到模板。 你只需将 location 属性更新为目标区域，如下一步所示。

8. 将主题资源的 location 更新为目标区域或位置。 区域的代码是不带空格的区域名称，例如 China North 3 等同于 chinanorth3。

```
"type": "Microsoft.EventGrid/topics",
"apiVersion": "2020-06-01",
"name": "[parameters('topics_yoz_eg_mts_name')]",
    "location": "chinanorth3",
```

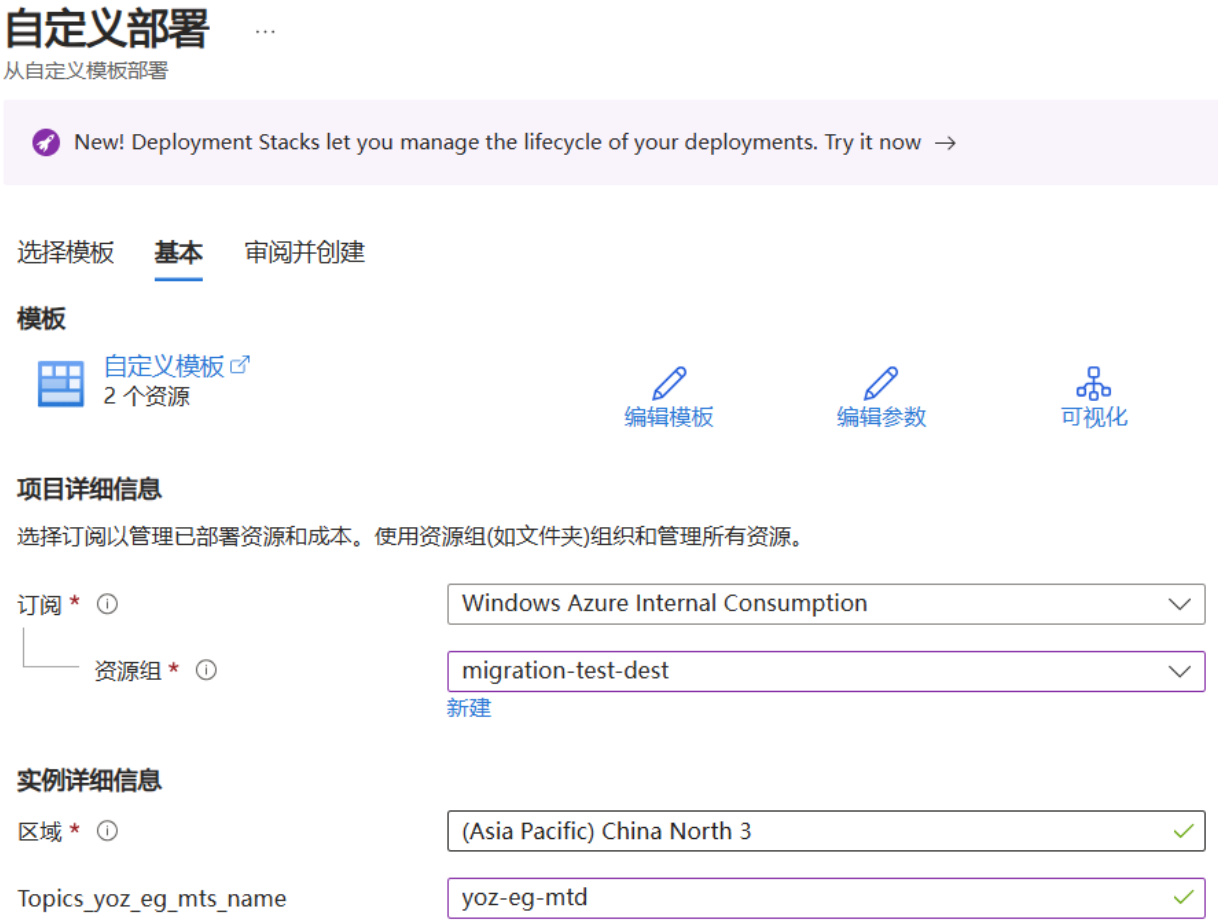
9. 保存该模板。

重新部署

部署该模板以在目标区域中创建自定义主题。

1. 在 Azure 门户中，选择“创建资源”。
2. 在“搜索市场”中键入“模板部署”，然后按 ENTER。
3. 选择“模板部署”。
4. 选择“创建” 。
5. 选择“在编辑器中生成自己的模板”。
6. 选择“加载文件”，然后按说明加载在上一部分下载的 template.json 文件。
7. 选择“保存”以保存该模板。
8. 在“自定义部署”页上执行以下步骤。
    1. 选择 Azure 订阅。
    2. 选择目标区域中现有的资源组，或者创建一个资源组。
    3. 对于“区域”，请选择目标区域。 如果选择了现有资源组，则此设置为只读。

4. 对于“主题名称”，请为该主题输入新名称。



5. 在页面底部选择“审阅并创建”。
6. 在“审阅并创建”页上查看基本信息，然后选择“创建” 。

验证

1. 部署成功后，选择“转到资源”。
2. 请确认看到了该自定义主题的“事件网格主题”页面。
3. 按照将向主题发送事件中的步骤，将事件发送到该主题。 验证是否调用了 Webhook 事件处理程序。

迁移 Azure Logic Apps

概述

Azure Logic Apps 是一个云平台，在该平台中创建和运行自动化工作流可以几乎不使用代码。 通过使用可视化设计器并从预生成的操作中进行选择，可以快速生成集成和管理应用、数据、服务和系统的工作流。Azure Logic Apps 可以选择创建"消耗"或"标准"逻辑应用工作流。

本文档旨在指导您如何将 Azure Logic Apps 从一个区域迁移到另一个区域。 ## 迁移准备工作

在开始迁移之前，请确保您具备以下条件：

- 创建要移动的逻辑应用或集成帐户时所用的同一个 Azure 订阅
- 拥有移动和设置所需资源的资源所有者权限。 深入了解 Azure 基于角色的访问控制 (Azure RBAC)。

注意事项

- 只能在 Azure 资源组或订阅之间移动特定的逻辑应用资源类型。
- 检查可在 Azure 订阅中和每个 Azure 区域中使用的逻辑应用资源数限制。 当不同订阅或资源组所在的区域相同时，这些限制会影响到能否移动特定的资源类型。 例如，对于每个 Azure 区域中的每个 Azure 订阅，只能使用一个免费层集成帐户。
- 移动资源时，Azure 将创建新的资源 ID。 因此，请确保改用新的 ID，并更新与所要移动的资源关联的任何脚本或工具。
- 在订阅、资源组或区域之间迁移逻辑应用之后，必须重新创建或重新授权任何需要 Open Authentication (OAuth) 的连接。
- 只能将集成服务环境 (ISE) 移到同一 Azure 区域或 Azure 订阅中存在的另一个资源组。 不能将 ISE 移到另一个 Azure 区域或 Azure 订阅中存在的资源组。 此外，在此类移动之后，必须在逻辑应用工作流、集成帐户、连接等等中更新对 ISE 的所有引用。

迁移方案

- 更多信息请阅读 将逻辑应用资源移到其他 Azure 资源组、区域或订阅 文档中，关于 **在区域之间移动资源** 章节的描述

相关参考文档

- 通过完成逻辑应用教程，熟悉 Azure 逻辑应用中的功能。
- 查阅 Azure 逻辑应用概述。

Azure 计划程序作业

Azure 计划程序 已于 2022 年 1 月 31 日完全停用

如果您想了解更多，请阅读：

- Azure 计划程序将于 2022 年 1 月 31 日停用
- 将 Azure 计划程序作业迁移到 Azure 逻辑应用 相关内容

迁移 Azure Service Bus

在很多情况下，可能需要将现有服务总线命名空间从一个区域移到另一个区域。 例如，可能需要创建一个具有相同配置的命名空间，以便进行测试。 此外，还可能需要在另一个区域中再创建一个命名空间，作为灾难恢复计划的一部分。

下面是概要步骤：

1. 将当前区域中的服务总线命名空间导出到 Azure 资源管理器模板。
2. 更新模板中资源的位置。 此外，从模板中删除默认订阅筛选器，因为用户无法创建默认规则，系统会自动创建。
3. 使用该模板将服务总线命名空间部署到目标区域。
4. 验证部署，确保已在目标区域中创建命名空间、队列、主题和主题订阅。
5. 更新所有连接源区域 service bus 服务使用的 AccessKey 为目标区域的 AccessKey。

先决条件

确保目标区域支持帐户使用的 Azure 服务总线和功能。

准备

若要开始，请导出资源管理器模板。 此模板包含描述服务总线命名空间的设置。

1. 登录 Azure 门户。
2. 选择“所有资源”，然后选择你的服务总线命名空间。
3. 在“服务总线命名空间”页上，选择左侧菜单中的“自动化”下的“导出模版”。
4. 选择“导出模板”页中的“下载”。
5. 找到从门户下载的 .zip 文件，并将该文件解压缩到所选的文件夹。 此 zip 文件包含模板和参数 JSON 文件。
6. 在解压缩的文件夹中打开 template.json 文件。
7. 搜索 location，并将该属性的值替换为区域或位置的新名称。区域的代码是不带空格的区域名称，例如 China East 等同于 chinaeast。
8. 删除以下类型的资源定义：Microsoft.ServiceBus/namespaces/topics/subscriptions/rules。 别忘了删除此部分前面的逗号 (,) 字符，以确保 JSON 有效。

注意：不能使用资源管理器模板为订阅创建默认规则。 在目标区域中创建订阅时，系统将自动创建默认规则。

移动

部署模板以在目标区域中创建服务总线命名空间。

1. 使用自定义模板进行部署，模板使用上一步下载后的 template.json 文件。
2. 在“自定义部署”页上选择目标区域，并输入新的命名空间名称，点击创建。

验证

在部署成功后，选择“转到资源组”。

在“资源组”页上，选择“服务总线命名空间”。

在“服务总线命名空间”页上，验证是否可以看到源区域中的队列、主题和订阅。

1. 在右侧窗格底部的命名空间中可以看到“队列”。
2. 切换到“主题”选项卡，查看命名空间中的主题。
3. 选择主题，验证是否已创建订阅。

迁移 Azure Functions

Azure Functions 资源是特定于区域的，不能跨区域移动。 必须在目标区域中创建现有函数应用资源的副本，然后将函数代码重新部署到新应用。

如果需要最短停机时间，请考虑在两个区域中运行函数应用以实现灾难恢复体系结构：

- Azure Functions 异地灾难恢复
- Azure Durable Functions 中的灾难恢复和异地分布

先决条件

- 确保目标区域支持 Azure Functions 和要移动其资源的任何相关服务
- 有权访问要迁移的函数的原始源代码

准备

标识源区域上使用的所有函数应用资源，其中可能包括以下内容：

- 函数应用
- 托管计划
- 部署槽位
- TLS/SSL 证书和设置
- 配置网络选项
- 托管标识
- 配置的应用程序设置 - 具有足够访问权限的用户可以使用门户中的高级编辑功能来复制所有源应用程序设置
- 缩放配置

函数可以使用触发器或绑定连接到其他资源。 有关如何跨区域移动这些资源的信息，请参阅相应服务的文档。

还应该能够从现有资源导出模板。

移动

将函数应用部署到目标区域并查看配置的资源。

重新部署函数应用

如果有权访问在源区域中创建函数应用的部署和自动化资源，请在目标区域中重新运行相同的部署步骤以创建和重新部署应用。

如果只能访问源代码而不能访问部署和自动化资源，则可使用任何可用的部署技术在目标区域上部署和配置函数应用。

查看配置的资源

如果在部署期间未配置资源，请查看并配置在上述准备步骤中在目标区域中标识的资源。

移动注意事项

- 如果部署资源和自动化没有创建函数应用，请在目标区域中在新的托管计划中创建相同类型的应用
- 函数应用名称在 Azure 中全局唯一，因此目标区域中的应用不能与源区域中的应用名称相同
- 需要检查将函数应用连接到依赖项的引用和应用程序设置，并在需要时进行更新。 例如，移动函数调用的数据库时，还必须更新应用程序设置或配置以连接到目标区域中的数据库。 一些应用程序设置（例如 Application Insights 检测密钥或函数应用使用的 Azure 存储帐户）可能已经在目标区域中配置，不需要更新
- 请记住在目标区域验证配置并测试函数
- 如果配置了自定义域，请重新映射域名

清理源资源

移动完成后，从源区域中删除函数应用和托管计划。 即使高级计划或专用计划中的函数应用本身未运行，也需要为其付费。

有关更多信息

请参阅在 Azure Functions 中的区域之间移动函数应用

迁移 Azure Virtual Desktop

概述

Azure 虚拟桌面（Virtual Desktop）不支持跨区域迁移现有资源，需要通过导出源区域资源模板并在新区域中重新部署创建资源的方式进行迁移。

此过程中不执行实际资源移动。 相反会删除旧资源，并在目标区域重新创建这些资源。
建议在生产工作负荷上使用此过程之前对其进行测试，了解其如何对部署产生影响。

本文中的信息适用于所有 Azure 虚拟桌面资源，包括主机池、应用程序组、缩放计划和工作区。

重要信息

在不同区域之间移动 Azure 虚拟桌面资源时，应牢记以下几点：

- 导出资源时，必须将它们作为一个集移动。 与特定主机池关联的所有资源必须保持在一起。 主机池及其关联的应用程序组需要位于同一区域。
- 工作区及其关联的应用程序组也需要位于同一区域。
- 缩放计划和分配的主机池也需要处于同一区域。
- 所有要移动的资源都必须位于同一资源组中。 模板导出要求资源位于同一组中，因此，如果希望它们位于不同位置，则需要修改导出的模板以更改其资源的位置。
- 将资源移动到新区域后，必须删除原始资源。 在移动过程中，资源的资源 ID 不会更改，因此，如果不删除旧资源，会与其发生名称冲突。
- 附加到要移动的主机池的现有会话主机将停止工作。 你将需要在新区域中重新创建会话主机。

迁移

迁移流程步骤主要为： 1. 导出模板。 2. 修改导出的模板。 3. 删除原始资源。 4. 部署修改后的模板。

您可以参照 在区域之间移动 Azure 虚拟桌面资源中所描述的详细步骤，完成迁移过程。

总结

在生产环境迁移前，请先在测试环境进行测试验证。
如果遇到任何问题，可以参考 Azure 官方文档或联系 Azure 技术支持。

有关更多信息：

* Azure 虚拟桌面

* 有关移动资源后可在部署中使用的更多模板，请参阅 适用于 Azure 虚拟桌面的 Azure 资源管理器模板

迁移 Azure Batch 服务

目录

- 简介
- 先决条件
- 准备工作
- 迁移步骤
    - 导出模板
    - 修改模板
    - 创建 Batch 账户
    - 配置 Batch 账户
    - 数据迁移
    - 验证与测试
    - 清理资源
- 总结

简介

本手册旨在指导您如何将 Azure Batch 服务从一个区域迁移到另一个区域。我们将详细介绍迁移步骤和注意事项，确保迁移过程顺利完成。

在某些情况下，你可能想将现有 Azure Batch 服务从一个区域移到另一个区域。 例如，你可能想要迁移以实现灾难恢复计划。 虽然不能将 Azure Batch 服务直接从一个区域移到另一个区域，但可使用 Azure 资源管理器模板（ARM 模板）来导出 Azure Batch 服务的现有配置。 然后，利用 ARM 模板在另一个区域中创建 Azure Batch 服务。 首先，将 Azure Batch 服务配置导出模板文件。 接下来，修改模板文件参数以匹配目标区域。 然后，将修改后的模板部署到新区域。 最后，在 Azure Batch 服务中重新创建作业、作业计划、任务等。

先决条件

- 确保你的 Azure Batch 服务使用的服务和功能在新目标区域中可以支持。
- 建议将与 Batch 帐户关联的任何 Azure 资源移动到新目标区域。 例如，按照将 Azure 存储帐户移动到另一个区域中的步骤移动关联的 Azure 存储帐户。 如果需要，你可以将资源保留在原始区域，但是，如果 Batch 帐户与工作负载使用的其他 Azure 资源位于同一区域，则性能通常会更好。 本文假设已迁移存储帐户或任何其他区域 Azure 资源，以便与 Batch 帐户保持一致。

准备工作

在开始之前，请确保您已经具备以下条件：

1. 一个有效的 Azure 订阅。
2. 源区域和目标区域的权限。
3. Azure CLI 已安装且配置好。
4. 确保 Batch 服务没有正在处理的任务，并且数据已经备份。

迁移步骤

导出模板

导出包含 Batch 帐户设置和信息的 ARM 模板。

1. 登录到 Azure 门户。
2. 选择“所有资源”，然后选择你的 Batch 帐户。
3. 选择“设置”>“导出模板”。
4. 选择“包含参数”复选框。
5. 选择“导出模板”页中的“下载”。
6. 找到从 Azure 门户下载到本地的 .zip 压缩文件，并解压到本地。

   此 zip 压缩文件包含组成模板的 *template.json* 和 *parameters.json* 两个文件。

修改模板

加载并修改该模板，以便可以在目标区域创建新的 Azure Batch 服务。

1. 在 Azure 门户中，选择“创建资源”。
2. 在“搜索服务和市场”中键入“模板部署”，然后按 **ENTER**。
3. 选择“模板部署(使用自定义模板部署)”。
4. 选择“创建” 。
5. 选择“在编辑器中生成自己的模板”。
6. 选择“加载文件”，然后选择在上一节下载的 “*template.json*” 文件 。

7. 将如下代码中 “” 替换为目标 Batch 帐户名称 。

```
{
  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#
",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "batchAccounts_mysourceaccount_name": {
      "defaultValue": "<target-batch-account>",
      "type": "String"
    }
  },
```

8. 在目标区域创建 Azure 资源组和 Azure 存储账户。

9. 将如下代码中 “” 替换为目标订阅 ID，如在同一个订阅下操作无需替换。

   将如下代码中 “” 替换为目标资源组。

   将如下代码中 “” 替换为目标存储帐户。

```
  "storageAccounts_mysourcestorageaccount_externalid": {
      "defaultValue": "/subscriptions/<subscription-id>/resourceGroups/<target-resource-group>/provi
ders/Microsoft.Storage/storageAccounts/<target-storage-account>",
      "type": "String"
    }
},
```

10. 将如下代码中 “” 替换为目标区域。

```
 {
    "resources": [
      {
        "type": "Microsoft.Batch/batchAccounts",
        "apiVersion": "2021-01-01",
        "name": "[parameters('batchAccounts_mysourceaccount_name')]",
        "location": "<target-location>",
```

11. 修改完成后，选择 “*template.json*” 文件下面的“保存” 。

创建 Batch 帐户

1. 输入或选择属性值：

   - **订阅**：选择 Azure 订阅。
   - **资源组**：选择目标区域资源组。
   - **区域**：请选择要将 Batch 帐户移动到的 Azure 区域。

2. 依次选择 “查看并创建”>“创建” 。

配置 Batch 帐户

Batch 帐户中的某些功能不会导出到模板中，因此必须在新的 Batch 帐户中重新创建这些功能，包括：

- 作业（和任务）
- 作业计划
- 证书
- 应用程序包

请确保根据需要配置新帐户中的功能。 可以参考源 Batch 帐户来了解如何配置这些功能。

数据迁移

如果有数据需要迁移，例如存储在 Azure Storage 中的 Blob，将其复制到新的存储账户。

验证与测试

1. 启动新创建的 Batch 服务，并验证其配置是否正确。

```
# 列出新的 Batch 账户中的池和作业，以确保它们与旧账户中的信息匹配
az batch pool list `
--account-endpoint <NewBatchAccountEndpoint> `
--account-key <NewBatchAccountKey> `
--account-name <NewBatchAccountName>
# 列出新的 Batch 账户中的作业
az batch job list `
--account-endpoint <NewBatchAccountEndpoint> `
--account-key <NewBatchAccountKey> `
--account-name <NewBatchAccountName>
```

2. 部署测试任务，确保新的 Batch 服务能够正常处理作业。

清理资源

如果确认新的 Batch 服务正常运行，可以删除源区域的旧 Batch 服务和相关资源。

总结

通过以上步骤，您已经成功将 Azure Batch 服务从一个区域迁移到另一个区域。请确保在迁移过程中仔细检查每一步，以避免数据丢失或服务中断。如果遇到任何问题，可以参考 Azure 官方文档或联系 Azure 技术支持。

了解如何进行 Azure Batch 服务的迁移， 相关参考文档:

- Azure Batch 教程
- 在 Azure 门户中创建 Azure Batch 帐户
- 使用 ARM 模板创建 Azure Batch 帐户

如有任何问题，请联系您的 Azure 支持团队。

迁移 Azure Cloud Services

目录

- 简介
- 先决条件
- 准备工作
- 迁移步骤
    - 停止云服务
    - 准备配置和包文件
    - 在目标区域创建云服务
    - 验证与测试
    - 清理资源
- 总结

简介

本文介绍 **Azure 云服务（外延支持）** 从一个区域迁移到另一个区域的方案。目前还不支持将 Azure 云服务（外延支持）从一个 Azure 区迁移到另一个区域，因此我们提供的方案是利用服务定义 *(.csdef)* 、服务配置 *(.cscfg)* 和服务包 *(.cspkg)* 文件在目标区域重新部署 Azure 云服务（外延支持），从而实现将 Azure 云服务（外延支持）迁移到 Azure 目标区域 。

目前，**Azure 云服务（经典）已经弃用**，并于 2024 年 8 月 31 日对所有客户停用。参见 Azure 云服务（经典）概述。

如何将 Azure 云服务（经典）迁移到 Azure 云服务（外延支持），请参考 Azure 云服务相关的迁移概述。

先决条件

1. **虚拟网络**：Azure 云服务（外延支持）部署必须在虚拟网络中。 可以使用 Azure 门户、Azure PowerShell、Azure CLI 或 Azure 资源管理器模板（ARM 模板）来创建虚拟网络。 必须在配置 (.cscfg) 文件的 NetworkConfiguration 节中引用虚拟网络和子网。

   对于与云服务位于同一资源组中的虚拟网络，仅引用服务配置 (.cscfg) 文件中的虚拟网络名称已经足够。如果虚拟网络和云服务（外延支持）位于两个不同的资源组中，请在配置 (.cscfg) 文件中指定虚拟网络的完整 Azure 资源管理器 ID。

    - 同一资源组中的虚拟网络：

```
<VirtualNetworkSite name="<vnet-name>"/>
 <AddressAssignments>
  <InstanceAddress roleName="<role-name>">
   <Subnets>
    <Subnet name="<subnet-name>"/>
   </Subnets>
  </InstanceAddress>
 </AddressAssign
```

- 不同资源组中的虚拟网络：

```
<VirtualNetworkSite name="/subscriptions/<sub-id>/resourceGroups/<rg-name>/providers/
Microsoft.Network/virtualNetworks/<vnet-name>"/>
  <AddressAssignments>
   <InstanceAddress roleName="<role-name>">
    <Subnets>
    <Subnet name="<subnet-name>"/>
    </Subnets>
   </InstanceAddress>
  </AddressAssignments>
```

2. **访问控制**：包含网络资源的订阅必须具有 Azure 云服务（外延支持）“网络参与者”或更高角色。

3. **密钥保管库**：Azure 密钥保管库可存储与 Azure 云服务（外延支持）关联的证书。 将证书添加到密钥保管库，然后为部署引用配置文件 (.cscfg) 中的证书指纹。 还必须为**用于部署的 Azure 虚拟机**启用密钥保管库访问策略（在门户中），以便云服务（外延支持）资源可以检索作为机密存储在密钥保管库中的证书。 可以在 Azure 门户中创建密钥保管库，也可以使用 PowerShell 创建。 必须在与云服务相同的区域和订阅中创建密钥保管库。

准备工作

在开始之前，请确保您已经具备以下条件：

1. 一个有效的 Azure 订阅。
2. 已经启用了 Azure CLI，并且已经登录。
3. 迁移账号具有源区域和目标区域的权限。
4. 确保您的 Azure 云服务（外延支持）没有正在执行的任务，并且所有数据已备份。
5. 准备好最新的服务定义 *(.csdef)* 、服务配置 *(.cscfg)* 和服务包 *(.cspkg)* 文件。

迁移步骤

停止云服务

首先，停止您要迁移的 Azure 云服务（外延支持）资源。

```
az cloud-service power-off `
--resource-group <ResourceGroupName> `
--cloud-service-name <CloudServiceName>
```

准备配置和包文件

准备 Azure 云服务（外延支持）服务定义 *(.csdef)* 、服务配置 *(.cscfg)* 和服务包 *(.cspkg)* 文件，可以通过以下方式准备：

1. 找到源区域部署的 Azure 云服务（外延支持）资源对应的 Azure 存储帐户，在存储帐户容器可找到对应文件，进行下载。
2. 在 Visual Studio 找到对应 Azure 云服务（外延支持）项目，通过"打包"功能生成文件。

   以上要注意版本控制，验证当前文件版本与生产环境部署的一致。

在目标区域创建云服务

在 Azure 目标区域创建 Azure 云服务（外延支持）资源，可以通过以下方式创建：

1. 通过 Azure 门户部署 Azure 云服务（外延支持），参见使用 Azure 门户部署云服务（外延支持）。
2. 通过 Azure PowerShell 部署 Azure 云服务（外延支持），参见使用 Azure PowerShell 部署云服务（外延支持）。
3. 通过 ARM 模板部署 Azure 云服务（外延支持），参见使用 ARM 模板部署云服务（外延支持）。
4. 通过 SDK 部署 Azure 云服务（外延支持），参见使用 Azure SDK 部署云服务（外延支持）。

验证与测试

1. 启动新创建的 Azure 云服务（外延支持）并验证其状态。

```
az cloud-service show `
--resource-group <ResourceGroupName> `
--cloud-service-name <CloudServiceName>
```

2. 访问 Azure 云服务（外延支持）确保其正常运行，例如通过浏览器访问服务的 URL。

清理资源

确认新 Azure 云服务（外延支持）正常运行后，可以删除源区域的 Azure 云服务（外延支持）和相关资源。

```
az cloud-service delete `
--resource-group <ResourceGroupName> `
--cloud-service-name <CloudServiceName>
```

总结

通过以上步骤，您已经成功将 Azure 云服务（外延支持）从一个区域迁移到另一个区域。请确保在迁移过程中仔细检查每一步，以避免数据丢失或服务中断。如果遇到任何问题，可以参考 Azure 官方文档或联系 Azure 技术支持。

想进一步了解 Azure 云服务（外延支持） 内容， 请参考相关文档:

- Azure 云服务（经典）文档
- 将 Azure 云服务（经典）迁移到 Azure 云服务（外延支持）
- Azure 云服务（外延支持）文档

如有任何问题，请联系您的 Azure 支持团队。

迁移 Azure Virtual Machine

目录

- 概述
- 使用 Azure Resource Mover 进行虚拟机的迁移
  - 先决条件
  - 停机影响
  - 迁移流程
- 使用 Azure Site Recovery 进行虚拟机的迁移
- 总结

概述

本手册旨在指导您如何将 Azure 虚拟机（VM）从一个区域迁移到另一个区域。

您可以选择 使用 Azure Resource Mover 进行虚拟机的迁移 或者 使用 Azure Site Recovery 进行虚拟机的迁移 的方式进行迁移。

使用 Azure Resource Mover 进行虚拟机的迁移

若要将 Azure VM 移动到另一个区域，我们建议使用 Azure 资源转移器。 资源转移器提供以下功能： * 跨区域移动资源的单一中心。 * 缩短了移动时间并降低了复杂性。 你所需要的一切都在同一个位置。 * 移动不同类型的 Azure 资源的简单、一致的体验。 * 标识要移动的资源之间的依赖项的一种简单方法。 这有助于将相关资源移动到一起，以便在移动后，所有资源在目标区域中都按预期方式工作。 * 如果要在移动后删除源区域中的资源，请在源区域中自动清除它们。 * 测试。如果不想进行完整移动，可以尝试移动，然后将其丢弃。

首先，请先确认待迁移的 VM 是否为**加密的 VM**，因为是否加密的 VM 在迁移流程上会略有不同。

加密的 VM 可描述为： * 具有启用了 Azure 磁盘加密的磁盘的 VM。 有关详细信息，请参阅 使用 Azure 门户创建和加密 Windows 虚拟机。
* 使用客户管理的密钥 (CMK) 进行静态加密或服务器端加密的 VM。 有关详细信息，请参阅 使用 Azure 门户为托管磁盘启用使用客户管理的密钥进行服务器端加密。

先决条件

在开始之前，请先验证是否具备以下条件：

1. **资源移动器支持**

   查看支持的区域和其他常见问题。

2. **订阅权限**

   请检查你对包含待移动资源的订阅是否拥有“**所有者**”访问权限。

   > **为什么需要“所有者”访问权限?**

   > *首次为 Azure 订阅中的特定源和目标对添加资源时，资源转移器将创建受订阅信任的 系统分配的托管标识（以前称为托管服务标识 [MSI]）。*

   > *若要创建标识，并为其分配所需的角色（来源订阅中的参与者或用户访问管理员），用于添加资源的帐户需要对订阅的“所有者”权限。 详细了解 Azure 角色。*

3. **VM 支持**

   - 检查要移动的 VM 是否受支持。
   - 验证受支持的 Windows VM。
   - 验证受支持的 Linux VM 和内核版本。
   - 查看支持的计算、存储和网络设置。

4. **目标订阅**

   目标区域中的订阅需要足够的配额来创建要在目标区域中移动的资源。 如果没有配额，请请求上调限额。

5. **目标区域费用**

   验证与要将 VM 移动到的目标区域关联的定价和费用。 请使用定价计算器来帮助你。

对于 **加密的 VM**，还需要额外验证是否具备以下条件：

1. **密钥保管库要求（Azure 磁盘加密）**

   如果已为 VM 启用 Azure 磁盘加密，则需要源区域和目标区域中的密钥保管库。 有关详细信息，请参阅创建密钥保管库。

   对于源区域和目标区域中的密钥保管库，你需要以下权限：

   - 密钥权限：密钥管理操作（Get、List）和加密操作（Decrypt 和 Encrypt）
   - 机密权限：机密管理操作（Get、List 和 Set）
   - 证书（List 和 Get）

2. **磁盘加密集（使用 CMK 的服务器端加密）**

   如果使用的 VM 是利用 CMK 进行服务器端加密的，则需要源区域和目标区域中的磁盘加密集。 有关详细信息，请参阅创建磁盘加密集。

   如果将硬件安全模块（HSM 密钥）用于客户管理的密钥，则不支持在区域之间移动。

停机影响

在启动移动阶段，会在目标区域中创建 副本 VM。 过程中可能会导致 源 VM 关闭，并出现一段停机时间（通常为几分钟）。

下表汇总了跨区域移动时受影响的内容。

行为	跨区域
数据	移动资源数据和元数据。 将暂时存储元数据，以跟踪资源依赖项和操作的状态。
资源	源资源保持不变以确保应用继续工作，可以选择在移动后将其删除。在目标区域中创建资源。
移动过程	需要手动干预和监视的多步骤过程。
测试	对移动进行测试非常重要，因为在移动后，应用应当继续在目标区域中按预期方式工作。
故障时间	预计不会丢失数据，但需要停机一段时间来移动资源。

更多有关于移动区域过程、状态以及移动影响相关的内容，请参阅关于移动过程。

迁移流程

根据 源 VM 是否为 **加密的 VM**，您可以参照 使用 Azure 资源转移器 跨区域移动 VM 或 跨区域移动加密的 Azure VM 中所描述的步骤完成虚拟机的迁移。

使用 Azure Site Recovery 进行虚拟机的迁移

由于目前中国所有 Azure 区域都处于 Azure 站点恢复（ASR） 所支持的相同地理集群（关于地理群集，请参阅）。

您还可以参照 将 VM 移动到另一个 Azure 区域 所描述的步骤完成虚拟机的迁移。

但我们更建议您 使用 Azure Resource Mover 进行虚拟机的迁移。

总结

请确保在迁移开始前仔细完整的阅读文档，并在过程中仔细检查每一步，以避免数据丢失或服务中断。

在生产环境迁移前，请先在测试环境进行测试验证。

如果遇到任何问题，可以参考 Azure 官方文档或联系 Azure 技术支持。

更多有关于 Azure VM 的参考文档：

- Azure 中的虚拟机

迁移 Azure Virtual Machine Scale Sets (VMSS)

简介

若要跨 Azure 区域迁移虚拟机规模集(VMSS)，请先导出资源管理器模板，并根据新环境对其进行调整，然后再重新部署到目标区域。

只需导出基本模板并在新环境中重新部署模板。各个虚拟机规模集实例都应该相同。

在开始重新部署之前，请确保了解对其他资源的依赖关系并将其迁移到目标区域。

重要事项

更改位置、密钥保管库机密、证书和其他 GUID，使其与新区域保持一致。

前提条件

在开始之前，请确保您具备以下前提条件：

- 如果源虚拟机支持可用区，则目标区域也必须支持可用区。要查看哪些区域支持可用区，请参阅 Azure 可用区支持的区域。
- 目标区域的订阅需要有足够的配额来创建资源。如果超出配额，请请求增加。有关详细信息，请参阅 Azure 订阅和服务限制、配额和约束。
- 整合源虚拟机规模集的所有相关扩展，因为某些需要在迁移后重新配置。
- 确认虚拟机映像是否为虚拟机映像库的一部分。库资源需要复制到目标区域。
- 捕获正在配置的资源列表，例如捕获诊断日志。这在优先级和排序上非常重要。
- 如果源区域 VMSS 依赖以下资源，请确保所依赖资源在目标区域可用并已部署：
    - 日志分析工作区
    - 诊断虚拟机规模集
    - Key Vault
    - 邻近放置组
    - 公共 IP 地址
    - 负载均衡器
    - 虚拟网络
- 确保您拥有网络贡献者角色或更高权限以在其他区域配置和部署负载均衡器模板。
- 确定源区域的解决方案网络布局，例如 NSG、公用 IP、VNet 地址空间等。

迁移

跨地域迁移虚拟机规模集的大致步骤如下： 1. 手动将源虚拟机规模集实例数设置为 0。 2. 导出源虚拟机规模集模板。 3. 根据新环境对模板内容进行调整。 4. 在目标区域，使用 IAC（基础设施即代码）工具（如 Azure 资源管理器模板、Azure CLI 或 PowerShell）使用导出的模板重新创建虚拟机规模集。 5. 将依赖资源关联到目标虚拟机规模集，例如 监控 部分中的日志分析工作区。同时，配置在 前提条件 部分 中整合的所有扩展。

更多详细操作请参考 将 Azure 虚拟机规模集重新定位到另一个区域

停机影响

在迁移过程中，需要注意以下停机影响：

- **实例停机：** 迁移过程中需要手动将源虚拟机规模集实例数设置为 0，这会导致实例停机，从而影响应用的可用性。
- **依赖资源重配置：** 在目标区域重新配置依赖资源可能导致短暂的服务中断，具体取决于资源的复杂性和数量。
- **数据同步延迟：** 如果涉及到数据迁移，可能会导致数据暂时不同步，影响实时性。

为减少停机影响，建议在迁移前做好以下准备： - **备份数据：** 确保在迁移前备份所有关键数据。 - **选择非高峰时间：** 在业务低峰期进行迁移，以最小化对用户的影响。 - **测试环境验证：** 先在测试环境中进行完整的迁移测试，验证所有步骤和配置。

总结 在生产环境迁移前，请先在测试环境进行测试验证。

如果遇到任何问题，可以参考 Azure 官方文档或联系 Azure 技术支持。

有关更多信息： * 通过完成 虚拟机规模集教程 来刷新您的知识。 * 了解如何 导出 Azure 资源管理器模板。 * 查阅 Azure 资源管理器概述。 * 获取 虚拟机规模集概述。 * 阅读 Azure 区域概述。 * 了解如何 重新部署模板。

迁移 Azure Application Gateway

本文介绍在 Azure 区域之间迁移应用程序网关的建议方法。

注意：本文档中的重新部署步骤仅适用于应用程序网关本身，而不适用于应用程序网关规则将流量路由到的后端服务。

注意：如果现有部署在 China North 区域的 V1 实例要迁移到其他区域，需要升级到 V2。

先决条件

- 确认 Azure 订阅允许在目标区域中创建应用程序网关 SKU。
- 先了解应用程序网关所需的所有服务再规划迁移策略。 必须对于迁移涉及的服务选择适当的迁移策略。
    - 应确保目标位置的应用程序网关子网有足够的地址空间来容纳处理最大预期流量所需的实例数。
- 对于应用程序网关的部署，必须考虑并规划以下子资源的设置：
    - 前端配置（公共/专用 IP）
    - 后端池资源（例如 VM、虚拟机规模集，Azure 应用服务）
    - 专用链接
    - Certificates
    - 诊断设置
    - 警报通知
- 应确保目标位置的应用程序网关子网有足够的地址空间来容纳处理最大预期流量所需的实例数。

重新部署

若要迁移应用程序网关，必须在目标位置使用新的公共 IP 地址创建单独的应用程序网关部署。 然后将工作负载从原来的应用程序网关设置迁移到新设置。 由于要更改公共 IP 地址，因此需要更改 DNS 配置、虚拟网络和子网。

如果只是为了获得可用性区域支持而迁移，请参阅将应用程序网关和 WAF 迁移到可用性区域支持。

若要创建单独的应用程序网关、WAF（可选）和 IP 地址：

1. 转到 Azure 门户。
2. 如果为密钥保管库使用 TLS 终止，请按照密钥保管库的迁移程序进行操作。 确保密钥保管库与被迁移的应用程序网关位于同一订阅中。 可以为被迁移的应用程序网关创建新证书或使用现有证书。
3. 在迁移*之前*，请确认虚拟网络已迁移。 若要了解如何迁移虚拟网络，请参阅迁移 Azure 虚拟网络。
4. 在迁移*之前*，确认后端池服务器或 VM、虚拟机规模集、PaaS 等服务已迁移。

5. 创建应用程序网关并为虚拟网络配置新的前端公共 IP 地址：
    - 无 WAF：创建应用程序网关
    - 有 WAF：使用 Web 应用程序防火墙创建应用程序网关
6. 如果有 WAF 配置或仅限自定义规则的 WAF 策略，将配置或策略转换为完整的 WAF 策略。
7. 如果具有 Azure 防火墙和应用程序网关的 Web 应用程序使用零信任网络（源区域），请遵循具有 Azure 防火墙和应用程序网关的 Web 应用程序零信任网络中的指引和策略。
8. 确认应用程序网关和 WAF 正常工作。
9. 将配置迁移到新的公共 IP 地址。
    1. 切换公共终结点和专用终结点以指向新的应用程序网关。
    2. 将 DNS 配置迁移到新的公共和/或专用 IP 地址。
    3. 更新使用者应用程序/服务中的终结点。 通常通过更改属性和重新部署来更新使用者应用程序/服务。 但是，如果在旧区域部署中使用新的主机名，请务必执行此方法。
10. 删除源头的应用程序网关和 WAF 资源。

迁移 Azure Bastion 资源

本指南将帮助您将 Azure Bastion 资源从一个区域迁移到另一个区域。由于 Azure Bastion 资源不支持直接跨区域迁移，您需要手动重新创建资源并更新相关配置。

迁移前准备

1. **规划新的网络设计**：评估目标区域的网络架构，确保其适合新的 Azure Bastion 资源，确定目标区域的虚拟网络 (VNet) 和子网配置。
2. **备份配置**：记录当前 Azure Bastion 配置，包括虚拟网络 (VNet)、子网、网络安全组(NSG)等。
3. **权限检查**：确保您有足够的权限在源区域和目标区域创建和管理 Azure 资源。

迁移步骤

1. 在目标区域创建新的 Azure Bastion

请阅读 教程：使用指定的设置部署 Azure Bastion

2. 更新虚拟网络和子网配置

1. 更新目标区域的虚拟网络配置以适用新的 Azure Bastion。
2. 如果需要，更新网络安全组(NSG)规则以允许必要的流量。

3. [可选] 使用虚拟网络对等互连

如果需要使用新的 Azure Bastion 连接原有资源，可以了解 虚拟网络对等互连和 Azure Bastion 的相关知识。

4. 测试连接

1. 使用新的 Azure Bastion 资源连接到虚拟网络中的虚拟机，确保连接正常。

5. 删除源区域的 Azure Bastion 资源

1. 确认目标区域的 Azure Bastion 资源工作正常后，您可以删除源区域的 Bastion 资源以避免额外费用。
2. 导航到源区域的 Bastion 资源，点击 **删除**。

常见问题

1. **是否可以直接迁移 Azure Bastion 资源?**

   不可以，Azure Bastion 资源不支持直接跨区域迁移。必须手动在目标区域重新创建并配置。

2. **如何确保迁移过程中没有数据丢失?**

   Azure Bastion 本身不存储数据，但确保虚拟网络和子网配置正确，以防止连接问题。

3. **迁移后，Public IP 是否可以保留?**

   不可以，Public IP 地址是区域性资源，无法跨区域迁移。因此，在目标区域创建新的 Azure Bastion 资源时，您需要分配一个新的 Public IP 地址。确保在迁移前通知相关方 IP 地址变更，以避免连接中断。

相关参考文档

Azure Bastion 文档

迁移 Azure DNS

概述

要将您的 Azure DNS 配置迁移到不同的 Azure 区域，您需要先导出 DNS 区域文件，然后在新的订阅下导入该文件。目前，导出和导入区域文件的唯一通用的方法是使用 Azure CLI。

停机时间

要了解可能涉及的停机时间，请参阅 面向 Azure 的云采用框架：选择迁移方法。

准备

1. 识别所有使用 Azure DNS 的 Azure 服务、应用程序和服务器。
2. 识别如何联系您的域名注册商并重新委派 NS 记录（如果需要）。

迁移步骤

Azure 公共 DNS

1. 登录到源 Azure 区域的源订阅，配置 Azure CLI 以使用 Azure 资源管理器模式。
2. 通过运行以下命令导出区域：

```
az network dns zone export -g <resource group> -n <zone name> -f <zone file name>
```

示例：

```
az network dns zone export -g "myresourcegroup" -n "contoso.com" -f "contoso.com.txt"
```

此命令调用 Azure DNS 服务以导出资源组 myresourcegroup 中的 contoso.com 区域。输出作为 BIND 兼容的区域文件存储在当前文件夹中的 contoso.com.txt 中。

3. 导出完成后，从区域文件中删除 NS 记录。新的 NS 记录将为新区域和订阅创建。
4. 登录到目标环境，创建一个新的资源组（或选择一个现有的资源组）。
5. 导入区域文件：

```
az network dns zone import -g <resource group> -n <zone name> -f <zone file name>
```

6. 导入区域后，您必须通过运行以下命令来验证区域：

```
az network dns record-set list -g <resource group> -z <zone name>
```

7. 验证完成后，联系您的域名注册商并重新委派 NS 记录。要获取 NS 记录信息，请运行以下命令：

```
az network dns record-set ns list -g <resource group> -z --output json
```

Azure 专有 DNS

1. 登录到源 Azure 区域的源订阅，配置 Azure CLI 以使用 Azure 资源管理器模式。
2. 通过运行以下命令导出区域：

```
az network private-dns zone export -g <resource group> -n <zone name> -f <zone file name>
```

示例：

```
az network private-dns zone export -g "myresourcegroup" -n "contoso.com" -f "contoso.com.txt"
```

此命令调用 Azure DNS 服务以导出资源组 myresourcegroup 中的 contoso.com 区域。输出作为 BIND 兼容的区域文件存储在当前文件夹中的 contoso.com.txt 中。

3. 导出完成后，从区域文件中删除 NS 记录。新的 NS 记录将为新区域和订阅创建。
4. 登录到目标环境，创建一个新的资源组（或选择一个现有的资源组）。
5. 导入区域文件：

```
az network private-dns zone import -g <resource group> -n <zone name> -f <zone file name>
```

6. 导入区域后，您必须通过运行以下命令来验证区域：

```
az network private-dns record-set list -g <resource group> -z <zone name>
```

注意事项

- Azure DNS 支持通过 Azure CLI 和 Microsoft Azure 门户导入和导出区域文件。
- Azure 专用 DNS 支持通过 Azure CLI 导入和导出区域文件。 目前不支持通过 Azure PowerShell 或 Azure 门户导入区域文件。

参考内容

- 通过完成以下任务来刷新您的知识 Azure DNS 文档。
- 审查以下内容 Azure DNS 概述。
- 了解更多信息 Azure 公共 DNS 导入和导出。
- 了解更多信息 Azure 专有 DNS 导入和导出。

迁移 Azure ExpressRoute 实例

概述

目前不支持跨 Azure 区域迁移 Azure ExpressRoute 实例。对于跨云类型的迁移，我们建议您在目标 Azure 区域中创建新的 ExpressRoute 线路和新的 ExpressRoute 网关。

先决条件

在进行 Azure ExpressRoute 迁移之前，请确保您已经完成以下先决条件：

1. **网络拓扑图**：
    - 准备当前网络拓扑图和目标网络拓扑图，以便更好地规划迁移过程。
2. **确认服务提供商支持**
    - 确认您的服务提供商是否支持目标 Azure 区域中的 ExpressRoute 服务。某些服务提供商可能仅在特定地区提供服务或有不同的覆盖范围。 >标准 ExpressRoute SKU 不支持跨地缘政治区域的连接。 需要启用 ExpressRoute 高级版附加组件才能支持全球连接。 不支持从世纪互联运营的 Azure 连接到其他 Azure 云环境。 如有需要，请联系连接服务提供商。
3. **通知相关方**：
    - 通知所有受影响的用户和团队，并安排好迁移窗口。
4. **测试环境**：
    - 在测试环境中模拟迁移过程，确保一切顺利。

相关参考文档

- 通过完成 ExpressRoute 教程来刷新您的知识。
- 了解如何创建新的 ExpressRoute 网关。
- 了解 ExpressRoute 位置和服务提供商。
- 阅读有关 ExpressRoute 的虚拟网络网关的内容。

迁移 Azure Public IP

概述

公有 IP 地址资源可以迁移，但是该资源的公有 IP 地址会重新分配成新的 IP 地址。

如果需要移动绑定公有 IP 地址的云服务资源，例如虚拟机，可参阅相关迁移文档，例如：

- 通过 Azure 资源转移器跨区域移动 Azure VM | Azure Docs

注意：绑定公有 IP 地址的云服务资源迁移后将分配一个新的公有 IP 地址，请根据实际情况更新相关资源。

迁移 Azure 路由服务器实例

概述

目前不支持跨 Azure 区域迁移 Azure 路由服务器 实例。我们建议您在目标 Azure 区域中创建新的 Azure 路由服务器。

停机时间

如果在包含虚拟网络网关（ExpressRoute 或 VPN）的虚拟网络中创建或删除路由服务器，预计在操作完成之前会出现停机。

准备

1. 准备目标区域的网络拓扑，获取要与 Azure 路由服务器 建立 BGP 对等的 NVAs 部署拓扑和配置信息。

先决条件

在进行 Azure 路由服务器 迁移之前，请确保满足以下先决条件： 1. 目标区域的虚拟网络、虚拟网络网关、NVAs 已部署就绪。 2. NVAs 必须与 Azure 路由服务器部署在同一 VNet 或直接部署在 VNet 中的 NVAs 对等连接。 3. 如果需要与 Azure VPN 和 ExpressRoute 网关建立 BGP 对等，那么网关也需要部署在相同的虚拟网络中。 4. 在目标区域重新部署前，请参阅 Azure 路由服务器限制。

迁移步骤

1. 确保 Azure 路由服务器关联的资源已经在目标区域就绪。
2. 将 Azure 路由服务器重新部署到目标区域。
    - 使用 Azure 门户创建并配置路由服务器。
    - 使用 Azure PowerShell 创建并配置路由服务器。
    - 使用 Azure CLI 创建并配置路由服务器。
    - 使用 ARM 模板创建 Azure 路由服务器

参考内容

- 了解 什么是 Azure 路由服务器。
- 了解 教程：配置 Azure 路由服务器与网络虚拟设备 (NVA) 之间的 BGP 对等互连。
- 了解 排查 Azure 路由服务器问题。

迁移 Azure Traffic Manager

目录

- 简介
- 先决条件
- 准备工作
- 迁移步骤
  - 迁移终结点
  - 创建流量管理器配置文件
  - 验证与测试
  - 清理资源
- 总结

简介

目前不支持跨 Azure 区域迁移流量管理器配置文件。可通过在目标区域中创建新的流量管理器配置文件，然后在新的流量管理器中完成终结点等配置，从而实现跨 Azure 区域迁移流量管理器。

先决条件

- 确定源 Azure 流量管理器配置文件所在的区域。
- 确定相关资源是否需要跨 Azure 区域迁移，并做好迁移计划。
- 请验证 Azure 订阅是否允许在目标区域中创建流量管理器配置文件。 如有需要请联系支持部门，启用所需配额。
- 确保订阅提供足够的资源，以支持添加流量管理器配置文件。

准备工作

在开始之前，请确保您具备以下条件：

1. 一个有效的 Azure 订阅。
2. 源区域和目标区域的操作权限。
3. 确保您的流量管理器配置文件没有任何正在进行的任务，并且相关资源已经备份。

迁移步骤

迁移终结点

对于源流量管理器配置文件中每个终结点需要按照对应的迁移手册迁移到目标 Azure 区域。

创建流量管理器配置文件

您可以通过 Azure 门户或 ARM 模板在目标区域创建流量管理器配置文件。

1. 登录到 Azure 门户，然后选择“所有资源”。
2. 找到源流量管理器配置文件，并将其打开。
3. 选择“设置”>“导出模板”。
4. 选择“导出模板”页面顶端的“部署”。
5. 选择“编辑参数”，在联机编辑器中打开 *parameters.json* 文件。
6. 如果需要编辑流量管理器配置文件名称，请将“*<source-traffic-manager>*”替换为对应名称，请将名称括在引号中。
7. 如果需要编辑流量管理器对应终结点，请将“*<resource-id>*”替换为对应资源 ID，请将资源 ID 括在引号中。
8. 修改后在编辑器中选择“保存”。

```
{
  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentParameters.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "trafficManagerProfiles_source_tmconfig_name": {
      "value": "<source-traffic-manager>"
    },
    "sites_tm_webapp01_externalid": {
      "value": "<resource-id>"
    },
    "sites_tm_webapp02_externalid": {
      "value": "<resource-id>"
    }
  }
}
```

9. 选择“编辑模板”，在联机编辑器中打开 *template.json* 文件。
10. 如果需要更改终结点信息，请更改 **resources** > **endpoints** 下对应的属性值。

11. 在在线编辑器中选择“保存”。
12. 选择“基本信息”>“订阅”，选择要将流量管理器配置文件部署到的订阅。
13. 选择“基本信息”>“资源组”，选择要将流量管理器配置文件部署到的资源组。
14. 选择“基本信息”>“区域”，选择要将流量管理器配置文件部署到的区域。
15. 确认“基本信息”>“流量管理器配置文件”名称是否正确。
16. 确认“基本信息”>“终结点”资源 ID 是否正确。
17. 选择“审阅并创建”。
18. 选择“创建”以部署目标流量管理器配置文件。

验证与测试

1. 通过流量管理器配置文件中的 DNS 地址访问终结点进行验证测试。
2. 通过查询端点返回的监控指标，监控对源流量管理器配置文件的访问是否完全停止。有些 LDNS 可能已经缓存了旧的配置文件名称，在禁用源配置文件之前，最好等待一段时间以确保所有访问都路由到了新的流量管理器配置文件。

清理资源

禁用源流量管理器配置文件，在确定可以安全删除源流量管理器配置文件的情况下，可将其删除。

总结

通过以上步骤，您已经成功将 Azure Traffic Manager 配置文件从一个区域迁移到另一个区域。请确保在迁移过程中仔细检查每一步，以避免数据丢失或服务中断。如果遇到任何问题，可以参考 Azure 官方文档或联系 Azure 技术支持。

如想进一步了解 Azure Traffic Manager 迁移， 可参考相关文档:

- Azure Traffic Manager 概述
- Azure Traffic Manager 教程
- 创建新的 Azure Traffic Manager

如有任何问题，请联系您的 Azure 支持团队。

迁移 Web Application Firewall (WAF)

概述

若要迁移应用程序网关和 WAF（可选项），必须在目标位置 **使用新的公共 IP 地址** 创建单独的应用程序网关部署。然后将工作负载从原来的应用程序网关设置迁移到新设置。

先决条件

- 确认 Azure 订阅允许在目标区域中创建应用程序网关 SKU。
- 先了解应用程序网关所需的所有服务再规划迁移策略。 必须对于迁移涉及的服务选择适当的迁移策略。
    - 应确保目标位置的应用程序网关子网有足够的地址空间来容纳处理最大预期流量所需的实例数。
- 对于应用程序网关的部署，必须考虑并规划以下子资源的设置：
    - 前端配置（公共/专用 IP）
    - 后端池资源（例如 VM、虚拟机规模集，Azure 应用服务）
    - 专用链接
    - Certificates
    - 诊断设置
    - 警报通知
- 应确保目标位置的应用程序网关子网有足够的地址空间来容纳处理最大预期流量所需的实例数。

迁移步骤

请阅读 将 Azure 应用程序网关和 Web 应用程序防火墙 (WAF) 迁移到另一区域 以了解详细的迁移步骤。

相关参考文档

- Azure Application Gateway 文档

迁移 Azure Load Balancer

目录

- 简介
- 先决条件
- 准备工作
- 迁移步骤
    - 导出公共 IP 地址模板并部署到新区域
    - 导出负载均衡器模板并部署到新区域
    - 验证与测试
    - 清理资源
- 总结

简介

在某些情况下，可能需要将 Azure 上某个负载均衡器从一个区域迁移或复制到另一个区域。 例如，你可能想要创建另一个采用相同配置的负载均衡器进行测试。你还可能想要在灾难恢复规划过程中将负载均衡器移到另一个区域。

目前不支持跨 Azure 区域迁移负载均衡器实例。 但是，可以使用 Azure 资源管理器模板来导出负载均衡器的现有配置和公共 IP 地址。 然后，在 Azure 门户部署到另一区域，方法是：将负载均衡器和公共 IP 导出到某个模板，根据目标区域修改参数，然后将该模板部署到新区域。

先决条件

- 确保源 Azure 负载均衡器位于 Azure 的区域。
- 无法在 Azure 区域之间移动负载均衡器。 必须将新的负载均衡器关联到目标区域中的资源。
- 若要导出 Azure 负载均衡器配置，并部署模板在另一区域创建 Azure 负载均衡器，需要拥有“网络参与者”角色或更高级别的角色。
- 确定源网络布局和当前正在使用的所有资源。 此布局包括但不限于负载均衡器、网络安全组、公共 IP 和虚拟网络。
- 请验证 Azure 订阅是否允许在目标区域中创建负载均衡器。 如有需要请联系支持部门，启用所需配额。
- 确保订阅提供足够的资源，以支持添加负载均衡器。
- 如果您当前正在使用 Azure 负载均衡器 - **基础版**，则建议您升级到 Azure 负载均衡器 - **标准版**，参见 Azure 负载均衡器从“基本”升级到“标准”。

准备工作

在开始之前，请确保您具备以下条件：

1. 一个有效的 Azure 订阅。
2. 源区域和目标区域的权限。
3. Azure CLI 已安装且配置好。
4. 确保您的负载均衡器没有任何正在进行的任务，并且相关资源已经备份。

迁移步骤

导出公共 IP 地址模板并部署到新区域

1. 登录到 Azure 门户，然后选择“所有资源”。
2. 找到负载均衡器使用的“公共 IP 地址”，并将其打开。
3. 选择“设置”>“导出模板”。
4. 选择“导出模板”页面顶端的“部署”。
5. 选择“编辑参数”，在联机编辑器中打开 *parameters.json* 文件。
6. 若要编辑“公共 IP 地址”名称，请将源公共 IP 名称中 **parameters** 下的 **value** 属性值更改为目标公共 IP 地址的名称， 请将名称括在引号中。修改后在编辑器中选择“保存”。

```
  {
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
     "publicIPAddresses_myVM1pubIP_name": {
     "value": "<target-publicip-name>"
      }
     }
    }
```

7. 选择“编辑模板”，在联机编辑器中打开 *template.json* 文件。
8. 若要编辑要将公共 IP 移到的目标区域，请更改 **resources** 下的 **location** 属性值。

```
"resources": [
    {
    "type": "Microsoft.Network/publicIPAddresses",
    "apiVersion": "2019-06-01",
```

```
      "name": "[parameters('publicIPAddresses_myPubIP_name')]",
      "location": "<target-region>",
      "sku": {
        "name": "Standard",
        "tier": "Regional"
      },
      "properties": {
        "provisioningState": "Succeeded",
        "resourceGuid": "7549a8f1-80c2-481a-a073-018f5b0b69be",
        "ipAddress": "52.177.6.204",
        "publicIPAddressVersion": "IPv4",
        "publicIPAllocationMethod": "Static",
        "idleTimeoutInMinutes": 4,
        "ipTags": []
      }
      }
    ]
```

若要获取区域位置代码，请参阅 Azure 位置。 区域代码是不带空格的区域名称。

9. 还可以根据需求更改模板中的其他参数：

   - **SKU**：可以在配置中将“公共 IP 地址”的 SKU 从 standard 更改为 basic 或者从 basic 更改为 standard，只需在 *template.json* 文件中更改 **sku** 下的 **name** 属性值即可：

```
"resources": [
{
  "type": "Microsoft.Network/publicIPAddresses",
  "apiVersion": "2019-06-01",
  "name": "[parameters('publicIPAddresses_myPubIP_name')]",
  "location": "<target-region>",
  "sku": {
    "name": "<Standard/Basic>",
    "tier": "Regional"
  },
```

   - **可用性区域**：可以通过更改“区域”属性来更改“公共 IP 地址”的区域。 如果未指定区域属性，会将公共 IP 创建为无区域。 可以指定单个区域来创建区域公共 IP，也可指定全部 3 个区域来创建区域冗余公共 IP。

```
"resources": [
{
  "type": "Microsoft.Network/publicIPAddresses",
  "apiVersion": "2019-06-01",
  "name": "[parameters('publicIPAddresses_myPubIP_name')]",
  "location": "<target-region>",
  "sku": {
    "name": "Standard",
    "tier": "Regional"
```

```
  },
  "zones": [
     "1",
     "2",
     "3"
  ],
```

- **公共 IP 分配方法**和**空闲超时**： 可以通过将“publicIPAllocationMethod”属性值从“Static”更改为“Dynamic”，或者从“Dynamic”更改为“Static”，来更改公共 IP 分配方法。 可以通过将 **idleTimeoutInMinutes** 属性值更改为所需值来更改空闲超时值，默认值为 4。在在线编辑器中选择“保存”。

```
"resources": [
{
  "type": "Microsoft.Network/publicIPAddresses",
  "apiVersion": "2019-06-01",
  "name": "[parameters('publicIPAddresses_myPubIP_name')]",
  "location": "<target-region>",
  "sku": {
     "name": "Standard",
     "tier": "Regional"
  },
  "zones": [
     "1",
     "2",
     "3"
  ],
  "properties": {
     "provisioningState": "Succeeded",
     "resourceGuid": "7549a8f1-80c2-481a-a073-018f5b0b69be",
     "ipAddress": "52.177.6.204",
     "publicIPAddressVersion": "IPv4",
     "publicIPAllocationMethod": "Static",
     "idleTimeoutInMinutes": 4,
     "ipTags": []
```

10. 在在线编辑器中选择“保存”。
11. 选择“基本信息”>“订阅”，选择要将“公共 IP 地址”部署到的订阅。
12. 选择“基本信息”>“资源组”，以选择要将“公共 IP 地址”部署到的资源组。 可以选择“新建”来为目标公共 IP 创建新的资源组。 请确保所选名称与现有源公共 IP 的源资源组不同。
13. 确认“基本信息”>“区域”是否设置为正确的目标区域。
14. 在“设置”下，确认“公共 IP 地址”名称是否与先前在 *parameters* 编辑器中输入的名称相匹配。
15. 选择“审阅并创建”。

16. 选择“创建”以部署目标“公共 IP 地址”。

17. 如果已有另一个公共 IP 正用于所要移动的负载均衡器的出站 NAT，请重复上述步骤导出第二个出站公共 IP 并将其部署到目标区域。

导出负载均衡器模板并部署到新区域

1. 登录到 Azure 门户，然后选择“所有资源”。

2. 找到要迁移的“负载均衡器”并将其选中。

3. 选择“设置”>“导出模板”。

4. 选择“导出模板”下的“部署”。

5. 选择“编辑参数”，在联机编辑器中打开 *parameters.json* 文件。

6. 若要编辑“负载均衡器”名称的参数，请将“负载均衡器”名称的 **value** 属性值更改为期望的名称。 请将名称括在引号中。

```
"$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#
",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "loadBalancers_myLoadbalancer_ext_name": {
    "value": "<target-external-lb-name>"
},
    "publicIPAddresses_myPubIP_in_externalid": {
    "value": "<target-publicIP-resource-ID>"
},
```

7. 若要编辑“负载均衡器”的公共 IP 地址为在前面步骤中创建的“公共 IP 地址”的值，必须先获取该资源 ID，然后将其粘贴到 *parameters.json* 文件中。 获取 ID 步骤：

    1. 在另一个浏览器标签页或窗口中，登录到 Azure 门户并选择“资源组”。

    2. 找到前面步骤中创建的“公共 IP 地址”，打开该资源。

    3. 选择“设置”>“属性”。

    4. 在右侧，突出显示“资源 ID”并将其复制到剪贴板。 或者，可以选择“资源 ID”路径右侧的“复制到剪贴板”。

    5. 将资源 ID 粘贴到在另一个浏览器窗口或标签页中打开的“编辑参数”编辑器中的 **value** 属性值：

    ```
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParam
    eters.json#",
    ```

```
  "contentVersion": "1.0.0.0",
  "parameters": {
    "loadBalancers_myLoadbalancer_ext_name": {
    "value": "<target-external-lb-name>"
},
    "publicIPAddresses_myPubIP_in_externalid": {
    "value": "<target-publicIP-resource-ID>"
},
```

6. 选择“保存”。

8. 如果为负载均衡器配置了出站 NAT 和出站规则，那么此文件中会显示第三个条目，该条目对应于出站公共 IP 的外部 ID。 在**目标区域**中重复上述步骤以获取出站公共 IP 的 资源 ID。 将该资源 ID 粘贴到 *parameters.json* 文件中：

```
"$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "loadBalancers_myLoadbalancer_ext_name": {
        "value": "<target-external-lb-name>",

    },
        "publicIPAddresses_myPubIP_in_externalid": {
        "value": "<target-publicIP-resource-ID>",

    },
        "publicIPAddresses_myPubIP_out_externalid": {
        "defaultValue": "<target-publicIP-outbound-resource-ID>",

    }
  },
```

9. 选择“模板”>“编辑模板”，在联机编辑器中打开 *template.json* 文件。

10. 若要编辑外部负载均衡器配置将要移到的目标区域，请更改 *template.json* 文件中 **resources** 下的 **location** 属性：

    若要获取区域位置代码，请参阅 Azure 位置。 区域代码是不带空格的区域名称。

```
"resources": [
    {
        "type": "Microsoft.Network/loadBalancers",
        "apiVersion": "2019-06-01",
        "name": "[parameters('loadBalancers_myLoadBalancer_name')]",
        "location": "<target-external-lb-region>",
        "sku": {
            "name": "Standard",
```

```
            "tier": "Regional"
        },
```

11. 还可以根据要求和需求更改模板中的其他参数：

    - **SKU**：可以在配置中将“负载均衡器”的 SKU 从“标准”更改为“基本”，或者从“基本”更改为“标准”，只需在 *template.json* 文件中更改“sku”下的 name 属性即可：

```
"resources": [
{
   "type": "Microsoft.Network/loadBalancers",
   "apiVersion": "2019-06-01",
   "name": "[parameters('loadBalancers_myLoadBalancer_name')]",
   "location": "<target-external-lb-region>",
   "sku": {
      "name": "Standard",
      "tier": "Regional"
   },
```

    - **负载均衡规则**： 可以通过在 *template.json* 文件的 **loadBalancingRules** 节中添加或删除条目，在配置中添加或删除负载均衡规则：

```
"loadBalancingRules": [
        {
            "name": "myInboundRule",
            "etag": "W/\"39e5e9cd-2d6d-491f-83cf-b37a259d86b6\"",
            "properties": {
                "provisioningState": "Succeeded",
                "frontendIPConfiguration": {
                    "id": "[concat(resourceId('Microsoft.Network/loadBalancers', parameters('loadBal
ancers_myLoadBalancer_name')), '/frontendIPConfigurations/myfrontendIPinbound')]"
                },
                "frontendPort": 80,
                "backendPort": 80,
                "enableFloatingIP": false,
                "idleTimeoutInMinutes": 4,
                "protocol": "Tcp",
                "enableTcpReset": false,
                "loadDistribution": "Default",
                "disableOutboundSnat": true,
                "backendAddressPool": {
                    "id": "[concat(resourceId('Microsoft.Network/loadBalancers', parameters('loadBal
ancers_myLoadBalancer_name')), '/backendAddressPools/myBEPoolInbound')]"
                },
                "probe": {
                    "id": "[concat(resourceId('Microsoft.Network/loadBalancers', parameters('loadBal
ancers_myLoadBalancer_name')), '/probes/myHTTPProbe')]"
                }
```

```
        }
      }
    ]
```

- **探测**：可以通过在 *template.json* 文件的 **probes** 节中添加或删除条目，在配置中添加或删除负载均衡器的探测：

```
"probes": [
      {
        "name": "myHTTPProbe",
        "etag": "W/\"39e5e9cd-2d6d-491f-83cf-b37a259d86b6\"",
        "properties": {
          "provisioningState": "Succeeded",
          "protocol": "Http",
          "port": 80,
          "requestPath": "/",
          "intervalInSeconds": 15,
          "numberOfProbes": 2
        }
      }
    ],
```

- **入站 NAT 规则**： 可以通过在 *template.json* 文件的 **inboundNatRules** 节中添加或删除条目，来添加或删除负载均衡器的入站 NAT 规则：

```
"inboundNatRules": [
      {
        "name": "myInboundNATRule",
        "etag": "W/\"39e5e9cd-2d6d-491f-83cf-b37a259d86b6\"",
        "properties": {
          "provisioningState": "Succeeded",
          "frontendIPConfiguration": {
            "id": "[concat(resourceId('Microsoft.Network/loadBalancers', parameters('loadBalancers_myLoadBalancer_name')), '/frontendIPConfigurations/myfrontendIPinbound')]"
          },
          "frontendPort": 4422,
          "backendPort": 3389,
          "enableFloatingIP": false,
          "idleTimeoutInMinutes": 4,
          "protocol": "Tcp",
          "enableTcpReset": false
        }
      }
    ]
```

若要完成某个入站 NAT 规则的添加或删除，该规则必须作为 **type** 属性出现在 *template.json* 文件的末尾，或者确认已经删除：

```
{
    "type": "Microsoft.Network/loadBalancers/inboundNatRules",
    "apiVersion": "2019-06-01",
    "name": "[concat(parameters('loadBalancers_myLoadBalancer_name'), '/myInboundNATRule')
]",
    "dependsOn": [
        "[resourceId('Microsoft.Network/loadBalancers', parameters('loadBalancers_myLoadBalanc
er_name'))]"
    ],
    "properties": {
        "provisioningState": "Succeeded",
        "frontendIPConfiguration": {
            "id": "[concat(resourceId('Microsoft.Network/loadBalancers', parameters('loadBalancers_
myLoadBalancer_name')), '/frontendIPConfigurations/myfrontendIPinbound')]"
        },
        "frontendPort": 4422,
        "backendPort": 3389,
        "enableFloatingIP": false,
        "idleTimeoutInMinutes": 4,
        "protocol": "Tcp",
        "enableTcpReset": false
    }
}
```

- **出站规则**：可以通过编辑 *template.json* 文件中的 **outboundRules** 属性，在配置中添加或删除出站规则：

```
"outboundRules": [
        {
            "name": "myOutboundRule",
            "etag": "W/\"39e5e9cd-2d6d-491f-83cf-b37a259d86b6\"",
            "properties": {
                "provisioningState": "Succeeded",
                "allocatedOutboundPorts": 10000,
                "protocol": "All",
                "enableTcpReset": false,
                "idleTimeoutInMinutes": 15,
                "backendAddressPool": {
                    "id": "[concat(resourceId('Microsoft.Network/loadBalancers', parameters('loadBal
ancers_myLoadBalancer_name')), '/backendAddressPools/myBEPoolOutbound')]"
                },
                "frontendIPConfigurations": [
                    {
                        "id": "[concat(resourceId('Microsoft.Network/loadBalancers', parameters('load
Balancers_myLoadBalancer_name')), '/frontendIPConfigurations/myfrontendIPoutbound')]"
                    }
                ]
```

```
        }
      }
    ]
```

12. 在编辑器中选择“保存”。

13. 选择“基本信息”>“订阅”，以选择要将负载均衡器部署到的订阅。

14. 选择“基本信息”>“资源组”，以选择要将负载均衡器部署到的资源组。 可以选择“新建”来为目标外部负载均衡器创建新的资源组。 请确保资源组名称与源负载均衡器的源资源组名称不同。

15. 确认“基本信息”>“区域”是否设置为负载均衡器部署的目标区域。

16. 在“设置”下，确认名称是否与先前在 parameters 编辑器中输入的名称相匹配。 确认是否为配置中的所有公共 IP 填充了资源 ID。

17. 选择“审阅并创建”。

18. 选择“创建”，完成负载均衡器的资源部署。

验证与测试

1. 启动并验证新创建的负载均衡器状态。

```
az network lb show `
--resource-group <TargetResourceGroupName> `
--name <TargetLoadBalancerName>
```

2. 测试新的负载均衡器配置是否正常工作。

清理资源

如果确认新负载均衡器正常运行，可以删除源区域的旧负载均衡器和关联资源。

```
az network lb delete `
--resource-group <ResourceGroupName> `
--name <LoadBalancerName>
```

总结

通过以上步骤，您已经成功将负载均衡器从一个区域迁移到另一个区域。请确保在迁移过程中仔细检查每一步，以避免数据丢失或服务中断。如果遇到任何问题，可以参考 Azure 官方文档或联系 Azure 技术支持。

进一步了解如何进行 Azure 负载均衡器的迁移， 请参考相关文档:

- Azure 负载均衡器概述
- Azure 负载均衡器教程
- 创建新的 Azure 负载均衡器
- Azure 负载均衡器从"基本"升级到"标准"

如有任何问题，请联系您的 Azure 支持团队。

迁移 Azure NAT 网关

概述

Azure NAT 网关是一种完全托管且高度可复原的网络地址转换 (NAT) 服务。 可以使用 Azure NAT 网关让专用子网中的所有实例出站能够连接到 Internet，同时保持完全专用。

NAT 网关实例不能直接从一个区域移至另一个区域。 一种解决方法是使用 Azure 资源转移器将与现有 NAT 网关关联的所有资源移至新区域。 然后，在新区域中创建 NAT 网关的新实例，然后将移动的资源与新实例关联。 在新的 NAT 网关在新区域中运行后，就可以删除之前区域中的旧实例。

停机时间

要了解可能涉及的故障时间，请参阅面向 Azure 的云采用框架：选择重定位方法。

相关参考文档

- 在将资源移至另一个区域后创建和配置 NAT 网关
- 快速入门：使用 Azure 门户创建 NAT 网关
- NAT 网关和可用性区域
- 使用 Azure NAT 网关设计虚拟网络

迁移 Azure Network Watcher

简介

Azure 网络观察程序（Network Watcher）本身不能直接从一个区域迁移到另一个区域。

网络观察程序是针对特定 Azure 区域启用的服务，用于监控和诊断网络流量。

我们建议您在目标区域中创建和配置新网络观察程序。然后，比较旧环境和新环境之间的结果。

总结

在生产环境迁移前，请先在测试环境进行测试验证。

如果遇到任何问题，可以参考 Azure 官方文档或联系 Azure 技术支持。

有关更多信息： * 查阅 网络观察程序概述。 * 了解有关 启用或禁用 Azure 网络观察程序的更多信息。 * 了解有关 网络安全组的流日志记录的更多信息。 * 阅读有关 连接监视器的内容。 * 查阅 网络观察程序的常见问题解答。 —

迁移 Azure 专有链接服务实例

概述

目前不支持跨 Azure 区域迁移 Azure 专有链接服务实例。我们建议您在目标 Azure 区域中创建新的专有链接服务。

停机时间

要了解可能涉及的停机时间，请参阅 面向 Azure 的云采用框架：选择迁移方法。

准备

1. 确定专用链接服务使用的所有资源，例如标准负载均衡器、虚拟机、虚拟网络、Azure PaaS 服务、Azure 专用 DNS 等服务。
2. 确定所有专有终结点的配置、专有 DNS 配置。

迁移步骤

针对标准负载均衡器后面的服务

1. 重新部署专用链接服务使用的所有资源。
2. 确保将具有所有依赖资源的标准负载均衡器迁移到目标区域。
3. 创建一个专有链接服务并引用迁移后的负载均衡器。要创建专用链接，可以使用 Azure 门户、PowerShell 或 Azure CLI。

   在负载均衡器选择过程中：

   - 选择要在其中接收流量的前端 IP 配置。
   - 选择专用链接服务的 NAT IP 地址的子网。
   - 选择与源专用链接服务相同的专用链接服务设置。
4. 将专用终结点重新部署到迁移后的虚拟网络中。
5. 按照专用 DNS 区域值中的指导配置 DNS 的设置。

针对 Azure PaaS 服务

1. 确保使用专有终结点的 Azure 服务已经迁移到目标区域。 有关支持专用链接的 Azure 服务的信息，请参阅 Azure 专用链接可用性。

2. 重新部署并使用专用终结点连接到 Azure 服务以开始使用 Azure 专用链接。关于如何为每个 Azure 服务创建专用终结点，请参阅相关 Azure 服务的教程。如，教程：使用专用终结点将 Azure Functions 与 Azure 虚拟网络集成。
3. 确保所有的专有终结点配置与专有 DNS 设置。

注意事项

在目标区域重新部署专有链接和专有终结点，建议采用新的资源组而不是同一个资源组，以避免冲突。

参考内容

- Azure 专用链接可用性
- 什么是 Azure 专用链接
- 什么是专用终结点

迁移 Azure Virtual Network

目录

- 简介
- 先决条件
- 准备工作
- 迁移步骤
    - 导出模板
    - 修改模板
    - 创建 Virtual Network
    - 配置 Virtual Network
    - 迁移关联资源
    - 验证与测试
    - 清理资源
- 总结

简介

目前不支持跨 Azure 区域迁移虚拟网络，我们建议您在目标区域中创建新的虚拟网络，并将资源迁移到这些虚拟网络中。

本手册旨在指导您如何将 Azure 虚拟网络（Virtual Network）从一个区域迁移到另一个区域。下文将介绍通过在新区域重新部署虚拟网络的方式实现虚拟网络跨区域迁移。 重新部署既支持多个工作负载的独立迁移，也支持目标区域的专用 IP 地址范围变化。 建议使用 ARM 资源管理器模板迁移虚拟网络。

先决条件

- 确定与迁移的虚拟网络关联的所有资源。
- 网络对等互连
    - 负载均衡器
    - 用户定义的路由 (UDR)
    - NAT 网关
    - DDOS 保护计划
    - 网络安全组 (NSG)
    - 保留专用 IP 地址（公共静态 IP 地址）

    - 应用程序安全组 (ASG)
- 确认虚拟网络位于源 Azure 区域中。
- 执行导出虚拟网络并部署模板，在另一区域创建虚拟网络的操作，需要“网络参与者”角色或更高级别的角色。
- 确定源网络布局和当前正在使用的所有资源。 此布局包括但不限于负载均衡器、网络安全组 (NSG) 和公共 IP。
- 验证 Azure 订阅是否允许在目标区域中创建虚拟网络。 若要启用所需配额，请联系支持部门。
- 了解以下注意事项：
    - 如果启用专用 IP 地址范围更改，则可以单独重新迁移虚拟网络中的多个工作负载。
    - 重新部署方法支持在目标区域中启用和禁用专用 IP 地址范围更改的选项。
    - 如果未在目标区域中启用专用 IP 地址更改，则只能使用公共端点（公共 IP 地址）建立需要在源区域和目标区域之间通信的数据迁移场景。

准备工作

在开始之前，请确保您已经具备以下条件：

1. 一个有效的 Azure 订阅。
2. 源区域和目标区域的权限。
3. Azure CLI 已安装并配置好。
4. 移动包含网络观察程序 NSG 日志的诊断存储帐户。
5. 重新定位网络安全组 (NSG)。
6. 禁用 DDoS 保护计划。

迁移步骤

导出模板

导出包含 Virtual Network 设置和信息的 ARM 模板。

1. 登录到 Azure 门户。
2. 选择“所有资源”，然后选择你的 Virtual Network。

3. 选择“设置”>“导出模板”。

4. 选择“包含参数”复选框。

5. 选择“导出模板”页中的“下载”。

6. 找到从 Azure 门户下载到本地的 .zip 压缩文件，并解压到本地。

   此 zip 压缩文件包含组成模板的 *template.json* 和 *parameters.json* 两个文件。

修改模板

加载并修改该模板，以便可以在目标区域创建新的 Virtual Network。

1. 在 Azure 门户中，选择“创建资源”。

2. 在“搜索服务和市场”中键入“模板部署”，然后按 **ENTER**。

3. 选择“模板部署（使用自定义模板部署）”。

4. 选择“创建”。

5. 选择“在编辑器中生成自己的模板”。

6. 选择“加载文件”，然后选择在上一节下载的 “*template.json*” 文件 。

7. 将如下代码中 “*<target-virtual-network-name>*” 替换为目标 Virtual Network 名称 。

```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "virtualNetworks_myVNET1_name": {
      "value": "<target-virtual-network-name>"
    }
  }
}
```

8. 将如下代码中 “*<target-region>*” 替换为目标区域。

```
"resources": [
        {
            "type": "Microsoft.Network/virtualNetworks",
            "apiVersion": "2019-06-01",
            "name": "[parameters('virtualNetworks_myVNET1_name')]",
            "location": "<target-region>",
            "properties": {
```

```
            "provisioningState": "Succeeded",
            "resourceGuid": "6e2652be-35ac-4e68-8c70-621b9ec87dcb",
            "addressSpace": {
              "addressPrefixes": [
                "10.0.0.0/16"
              ]
            },
```

9. 还可以根据需求更改模板中的其他参数：

- **地址空间**：修改 resources>addressSpace 节并更改 addressPrefixes 属性来更改虚拟网络的地址空间。

```
"resources": [
    {
    "type": "Microsoft.Network/virtualNetworks",
    "apiVersion": "2019-06-01",
    "name": "[parameters('virtualNetworks_myVNET1_name')]",
    "location": "<target-region",
    "properties": {
    "provisioningState": "Succeeded",
    "resourceGuid": "6e2652be-35ac-4e68-8c70-621b9ec87dcb",
    "addressSpace": {
      "addressPrefixes": [
      "10.0.0.0/16"
      ]
```

- **子网**：可以通过更改该模板的 subnets 节来更改子网名称和子网地址空间或在其中添加内容。 可以通过更改 **name** 属性来更改子网名称。 可以通过更改 **addressPrefix** 属性来更改子网地址空间。

```
"subnets": [
    {
    "name": "subnet-1",
    "etag": "W/\"d9f6e6d6-2c15-4f7c-b01f-bed40f748dea\"",
    "properties": {
    "provisioningState": "Succeeded",
    "addressPrefix": "10.0.0.0/24",
    "delegations": [],
    "privateEndpointNetworkPolicies": "Enabled",
    "privateLinkServiceNetworkPolicies": "Enabled"
    }
    },
    {
    "name": "GatewaySubnet",
    "etag": "W/\"d9f6e6d6-2c15-4f7c-b01f-bed40f748dea\"",
    "properties": {
    "provisioningState": "Succeeded",
    "addressPrefix": "10.0.1.0/29",
    "serviceEndpoints": [],
```

```
        "delegations": [],
        "privateEndpointNetworkPolicies": "Enabled",
        "privateLinkServiceNetworkPolicies": "Enabled"
      }
      }
    ]
```

10. 修改完成后，选择 “*template.json*” 文件下面的“保存” 。

创建 Virtual Network

1. 输入或选择属性值：
    - **订阅**：选择 Azure 订阅。
    - **资源组**：选择目标区域资源组。
    - **区域**：请选择要将虚拟网络移动到的 Azure 区域。
2. 依次选择 “查看并创建”、“创建” 。

配置 Virtual Network

虚拟网络中的某些配置不会导出到模板中，因此必须在新的虚拟网络中重新配置，包括但不限于如下项：

- Azure 防火墙
- 对等互联
- 服务终结点
- 专用终结点

请确保根据需要配置新虚拟网络中的设置。 可以参考源虚拟网络来了解如何配置这些功能。

迁移关联的资源

更改虚拟机和其他网络相关资源的配置，使其关联到新的虚拟网络。包括但不限于如下项：

- 虚拟机
- DNS 服务器
- 网络安全组

迁移方式参见相关资源迁移手册。

验证与测试

1. 确认所有资源都部署在新的虚拟网络中，并且所有配置都正确。
2. 验证虚拟机是否能够正确启动，并且配置无误。
3. 验证应用程序在新网络中的表现，确保正常运行。

清理资源

如果确认所有资源在新的区域中运行正常，可以删除旧的资源：

```powershell
# 删除源区域的虚拟网络
az network vnet delete `
--resource-group <ResourceGroupName> `
--name <VNetName>
```

总结

通过以上步骤，您已经成功将 Azure Virtual Network 从一个区域迁移到另一个区域。请确保在迁移过程中的每一步都仔细检查，以避免数据丢失或服务中断。如果遇到任何问题，可以参考 Azure 官方文档或联系 Azure 技术支持。

了解如何进行 Virtual Network 的迁移， 相关参考文档:

- Azure Virtual Network 概述
- Azure Virtual Network 教程
- Azure Virtual Network 规划

如有任何问题，请联系您的 Azure 支持团队。

迁移虚拟 WAN

概述

本指南将帮助您将 Azure 虚拟 WAN 从一个区域迁移到另一个区域。请注意，Azure 虚拟 WAN 本身不支持直接的区域迁移，因此需要手动重新创建和配置资源。

在大多数情况下，由于资源与网络密切相关，Azure 虚拟 WAN 在迁移过程中会对这些资源的使用产生影响。一个相对平滑的迁移方案是在新区域中创建一个新的 Azure 虚拟 WAN，并与当前的虚拟 WAN 进行互联。如果当前虚拟广域网下的虚拟网络（VNet）位于待迁移区域，则可以通过在其他区域新建虚拟网络的方式，详细迁移方案可以参考 Azure Virtual Network 区域迁移指南 的内容。迁移后将其连接到新的 Azure 虚拟 WAN 中，详细步骤可以参考 将虚拟网络连接到虚拟 WAN 中心 中的内容。如果原有的虚拟网络不在待迁移的区域，则需要断开与当前虚拟广域网中心（Hub）的连接，并重新连接到新的 Azure 虚拟广域网中。

Azure 虚拟 WAN 迁移过程中会导致网络暂时中断，因此需要提前做好规划和准备。

迁移前准备

- **评估和备份现有配置**
  - **评估现有的虚拟 WAN 配置**：全面检查当前虚拟 WAN 的设置，包括虚拟网络 (VNet)、连接、路由表、VPN 网关和 ExpressRoute 网关等信息。
  - **备份当前配置**：确保所有配置项都有备份，以便在迁移过程中或出现问题时能够快速恢复。特别注意备份虚拟网络、连接、路由表、VPN 网关和 ExpressRoute 网关的详细信息。
- **检查目标区域支持**
  - 确认目标区域支持所有需要的虚拟 WAN 功能和资源类型。有关详细信息，请参阅 虚拟 WAN 合作伙伴和位置 一文。
- **评估网络中断对业务的影响**
  - **业务影响分析**：识别哪些业务应用和服务依赖于当前的虚拟 WAN，并评估它们在迁移过程中可能受到的影响。确定对关键业务应用的潜在中断时长和可能的后果。
  - **利益相关者沟通**：与所有相关的团队和利益相关者（如业务部门、IT 运维团队、安全团队等）沟通，确保他们了解迁移计划和可能的网络中断时间。
  - **用户通知**：提前通知所有可能受影响的用户和客户，告知他们迁移的时间表和可能的服务中断。
- **制定应对措施**
  - **迁移窗口选择**：选择业务低峰期进行迁移，以最小化对业务运行的影响。
  - **临时解决方案**：为关键业务应用和服务准备临时解决方案或备用路径。例如，设置临时的 VPN 连接或使用其他网络服务来确保关键业务的连续性。

- **回滚计划**：制定详细的回滚计划，以防迁移过程中出现不可预见的问题。确保能够快速恢复到原有状态。

- **技术准备**
  - **测试迁移步骤**：在一个测试环境中模拟迁移过程，验证所有步骤和配置是否正确。确保新区域中的虚拟 WAN 和相关资源能够正常工作。
  - **监控和日志记录**：设置详细的监控和日志记录，以便在迁移过程中实时监控网络状态和性能。及时发现和解决可能的问题。

创建新的虚拟 WAN 并通过 VPN 连接

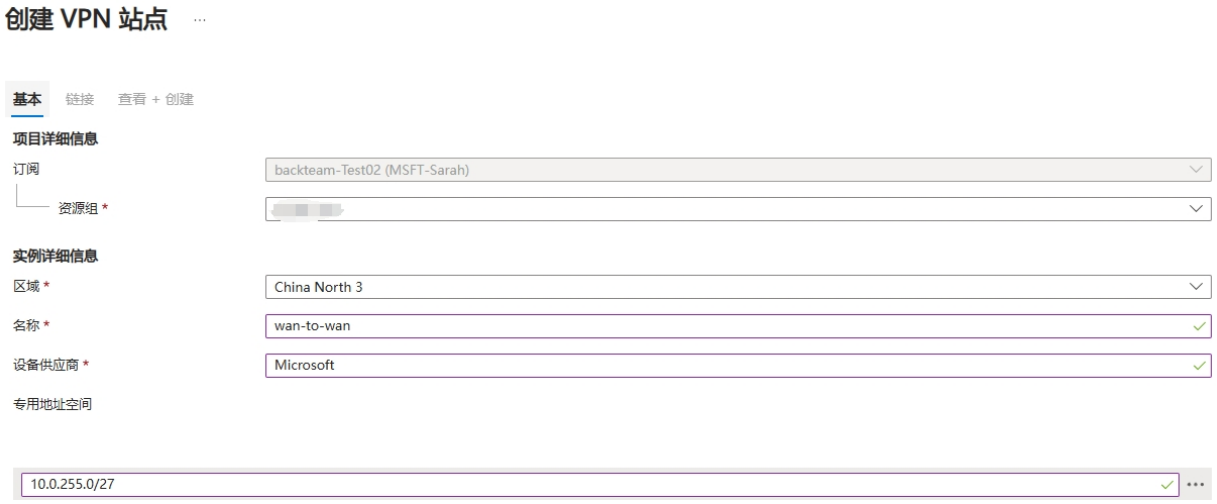
VPN 连接两个虚拟 WAN 是一个可选方法而不是必须方案。

1. 在新的区域中创建新的 Azure 虚拟 WAN

2. 创建新的 Hub

3. 配置站点到站点网关

4. 创建 VPN 站点



5. 添加链接。如果原有虚拟 WAN 没有创建 VPN Gateway，这里链接的 IP 地址可以写一个不存在的，后续我们会修改这里的配置

6. 在 Hub 中连接 VPN 站点

7. 创建好后获取 VPN Gateway Public IP 地址

8. 重复以上步骤，在原有的 Azure 虚拟 WAN 创建 VPN 站点及连接。
9. [可选]之前创建 VPN 链接时并没有使用正确的设置"链接 IP 地址",可以在原有 WAN 添加完后修正其地址。完成后检查连接状态

10. 测试两个 WAN 之间的网络连通性

迁移原区域 VNET

- Azure Virtual Network 区域迁移指南 的内容
- 将虚拟网络连接到虚拟 WAN 中心

迁移非原区域中的 VNET 到新的虚拟 WAN Hub 中

此操作会导致网络中断，请做好迁移前准备

1. 从原有 Hub 中删除

2. 添加到新的 Hub 中

相关参考文档

- 虚拟 WAN 文档
- 教程：使用 Azure 虚拟 WAN 创建站点到站点连接
- 教程：使用 Azure 虚拟 WAN 创建 P2S 用户 VPN 连接
- 教程：创建与虚拟 WAN 的 ExpressRoute 关联

迁移 Azure VPN 网关

概述

目前不支持跨 Azure 区域迁移 Azure VPN 网关实例。我们建议您在新区域中创建和配置 VPN 网关的新实例。
您可以使用门户网站或 PowerShell 收集有关当前 VPN 网关配置的信息。在 PowerShell 中，使用以 `Get-AbureRmVirtualNetworkGateway` 开头的一组 cmdlet。
确保更新您的本地配置。此外，在更新 Azure 网络环境后，删除旧 IP 地址范围内的任何现有规则。

先决条件

在进行 VPN Gateway 迁移之前，请确保您已经完成以下先决条件：

1. **备份配置**：
    - 确保备份当前 VPN Gateway 的所有配置，包括 IP 地址、子网、路由表和安全组等信息。
2. **访问权限**：
    - 确保您拥有足够的权限来创建、修改和删除 VPN Gateway 以及相关的资源。
3. **网络拓扑图**：
    - 准备当前网络拓扑图和目标网络拓扑图，以便更好地规划迁移过程。
4. **通知相关方**：
    - 通知所有受影响的用户和团队，并安排好迁移窗口。
5. **测试环境**：
    - 在测试环境中模拟迁移过程，确保一切顺利。

停机影响

在迁移过程中，可能会有以下停机影响：

1. **网络中断**：
    - 在切换到新的 VPN Gateway 时，可能会导致短暂的网络中断。
2. **服务不可用**：
    - 依赖于 VPN 连接的应用程序和服务可能会在迁移过程中不可用。
3. **用户连接中断**：
    - 远程用户的 VPN 连接可能会在迁移过程中中断，需要重新连接。

相关参考文档

- 通过完成 VPN 网关教程来刷新您的知识。
- 了解如何创建站点到站点的连接。
- 查阅 Az.Network VPN。
- 查阅 az network vnet 命令
- 阅读博客文章：创建站点到站点的连接。
- 查阅 Azure VPN Gateway 文档

迁移 Azure Container Registry

目录

- 简介
- 新建并导入
  - 先决条件
  - 服务终结点注意事项
  - 专用终结点注意事项
    - Azure 专用终结点 DNS 集成注意事项
  - 重新定位到另一个区域

简介

本指南旨在帮助您将 Azure Container Registry (ACR)从一个区域迁移到另一个区域。本指南基于使用 Azure CLI 进行操作。并特别针对 Azure 中国区域。

新建并导入

你可能需要将 Azure 容器注册表从一个 Azure 区域移到另一个 Azure 区域。 例如，你在一个不同的区域中运行开发管道或托管新的部署目标，并希望提供附近区域的注册表。

尽管 Azure 资源转移器无法自动对 Azure 容器注册表执行移动操作，但你可以手动将容器注册表移到另一个区域：

- 将注册表设置导出到资源管理器模板
- 使用模板在不同的 Azure 区域中部署注册表
- 将源注册表中的注册表内容导入到目标注册表

详细操作方式，请参考官方文档：将项目传输到另一个注册表

先决条件

使用手工方式转移区域，有如下先决条件：

- 只能在同一 Active Directory 租户中重新定位注册表。此限制适用于使用客户管理的密钥加密和解密的注册表。
- 如果源注册表启用了可用性区域，则目标区域也必须支持可用性区域。 有关对 Azure 容器注册表的可用性区域支持的详细信息，请参阅 启用 Azure 容器注册表中的区域冗余以实现复原能力和高可用性。

服务终结点注意事项

Azure 容器注册表的虚拟网络服务终结点将限制对指定虚拟网络的访问。 此外，还可通过这些终结点将访问限制为一系列 IPv4（Internet 协议版本 4）地址范围。 任何从外部连接到注册表的用户都无法访问这些资源。 如果在注册表资源的源区域中配置了服务终结点，则需要在目标区域中执行相同的操作。 下面介绍了此应用场景的步骤：

- 若要成功将注册表重新创建到目标区域，必须事先创建 VNet 和子网。 如果使用 Azure 资源转移器工具执行所有这些资源的移动，则不会自动配置服务终结点，并且你需要提供手动配置。
- 其次，需要在 Azure 容器注册表的 IaC 中进行更改。 在 networkAcl 部分中，在 virtualNetworkRules 下，添加目标子网的规则。 确保将 ignoreMissingVnetServiceEndpoint 标志设置为 False，从而实现以下效果：在目标区域中未配置服务终结点的情况下，IaC 无法部署 Azure 容器注册表。 这将确保满足目标区域中的先决条件

专用终结点注意事项

Azure 专用链接提供从虚拟网络到 Azure 平台即服务 (PaaS)、客户拥有的服务或 Microsoft 合作伙伴服务的专用连接。 专用链接简化了网络体系结构，并通过消除数据在公共 Internet 上的暴露来保护 Azure 中终结点之间的连接。

Azure 专用终结点 DNS 集成注意事项

请务必正确配置 DNS 设置，将专用终结点 IP 地址解析为连接字符串的完全限定的域名 (FQDN)。

现有 Microsoft Azure 服务可能已有针对公共终结点的 DNS 配置。 必须替代此配置才能使用专用终结点进行连接。

与专用终结点关联的网络接口包含配置 DNS 所需的信息。 网络接口信息包括专用链接资源的 FQDN 和专用 IP 地址。

可使用以下选项来配置专用终结点的 DNS 设置：

使用主机文件（仅推荐用于测试）。 可以使用虚拟机上的主机文件来替代 DNS。 使用专用 DNS 区域。 你可使用专用 DNS 区域来替代专用终结点的 DNS 解析。 可将专用 DNS 区域链接到你的虚拟网络，以解析特定域。 使用 DNS 转发器（可选）。 你可使用 DNS 转发器来替代专用链接资源的 DNS 解析。 创建 DNS 转发规则，以在虚拟网络中托管的 DNS 服务器上使用专用 DNS 区域。 必须在具有高级层的目标区域中配置 Azure 容器注册表。

禁用对注册表的公共网络访问后，某些受信任服务（包括 Azure 安全中心）对注册表的访问需要启用一个可绕过网络规则的网络设置。

如果注册表具有已批准的专用终结点且禁用了公共网络访问，则无法使用 Azure 门户、Azure CLI 或其他工具在虚拟网络外部列出存储库和标记。

对于新副本，必须手动为目标区域中的数据终结点添加新的 DNS 记录。

重新定位到另一个区域

对于注意事项的更详细的说明，可以参考国际版 Azure 的说明文档将 Azure 容器注册表重新定位到另一个区域，但请注意，国际版 Azure 和中国区 Azure 有所区别，此文档仅作参考。

迁移 Azure Service Fabric

目录

- 简介
- 准备工作
- 迁移步骤
  - 创建新 Service Fabric 集群
  - 迁移应用程序
  - 重定向流量
  - 验证与测试
  - 清理资源
- 总结

简介

Azure Service Fabric 群集资源的范围本质上局限在一个区域。 由此可见，群集资源不能跨区域移动，目前“跨区域移动”是这样完成的：首先在目标区域中创建一个新群集，然后迁移现有的应用程序，最后将流量定向到这个新的目标区域。 本文档概述了完成此迁移所需的步骤。 有几个决策点可以决定迁移的复杂程度。 这些输入包括如何设置并配置群集和应用程序，通信在群集中如何工作，以及工作负载是无状态、有状态还是两者都有。

本手册旨在指导您如何将 Azure Service Fabric 集群从一个区域迁移到另一个区域。我们将描述主要迁移步骤，以确保迁移过程顺利完成。

准备工作

在开始之前，请确保您已经具备以下条件：

1. 一个有效的 Azure 订阅。
2. 对源区域和目标区域的管理权限。
3. Azure CLI 已安装且配置好。
4. 在正式开始区域迁移之前，建议验证迁移方案和迁移步骤，并备份数据。
5. 阅读生产准备清单中推荐的指南。
6. 确保没有对 Service Fabric 群集资源的调用，也没有任何服务相互通信或执行处理。

迁移步骤

创建新 Service Fabric 集群

使用 Azure 门户或通过 Azure 资源管理器创建 Service Fabric 群集，参见使用 Azure 资源管理器创建 Service Fabric 群集。

通过针对群集和基础结构拓扑调整现有 ARM 模板，在新区域中设置一个群集。 如果当前没有描述群集的 ARM 模板，则建议从 Azure 资源浏览器检索当前 ARM 模板。 Azure 资源浏览器可帮助你发现当前已部署的资源及其配置信息，你可以使用这些资源和信息来创建一个或多个 ARM 模板，以便重复部署现有环境的克隆。 在继续操作之前，请测试并确认你具有可在此阶段部署现有环境克隆的可用 ARM 模板。

迁移应用程序

1. **通过 Azure 资源管理器将应用程序和服务部署到新的 Service Fabric 集群**，参见将应用程序和服务作为 Azure 资源管理器资源进行管理。

   请注意保留已执行的任何应用程序参数或配置自定义。 例如，如果应用程序有一个默认值为 5 的“count”参数，但你已在源环境中将该参数的值升级为 7，则需要确保该值在新区域的应用程序部署中也设置为 7。 如果你不使用 ARM 来管理应用程序和服务实例，则你要负责识别当前区域中运行的当前应用程序和服务集及其配置，并在新的区域/群集中复制这些应用程序和服务。

2. 迁移服务

   - 如果它是**有状态服务**，则需要将数据从旧群集移动到新群集。请参阅从旧群集备份数据，以了解如何将数据从旧群集移动到新群集的信息。对于有状态工作负载：

     - 为了确保有状态服务已经达到稳定点，请首先确保已停止向这些服务传入流量。 执行此操作的方式取决于将流量传递给你的服务的不同情况。 例如，可能必须从事件中心切断该服务，或者通过删除相应的路由或转发规则来阻止 APIM 或 Azure 网络负载均衡器等将流量路由到你的服务。 流量停止传入并且服务完成了与这些请求相关的后台处理后，可以继续操作。

     - 使用备份还原服务并执行按需备份，从任何有状态服务中进行备份，请确保在流量停止并且任何后台处理工作完成之后进行备份操作。 完成后，可将数据还原到新区域和群集中的有状态服务中。 用于执行备份的 Azure 存储帐户必须可供从新区域访问。

   - 如果它是**无状态服务**，则不需要移动数据，但您必须重新配置流量。对于无状态服务：

     - 除了将服务部署到新群集（最好是作为步骤 2 中完成的 ARM 应用程序部署的一部分）并确保它们的配置与源群集中的配置相同以外，不应该有额外的工作。

   - 对于所有服务：

- 更改部署到新区域里的应用程序配置。
- 确保客户端和服务之间任何通信阶段均配置为与源群集类似。 例如，此验证可能包括确保为事件中心、网络负载均衡器、应用程序网关或 API 管理等中介设置了允许流量流向群集所需的规则。

重定向流量

将流量从旧区域重定向到新区域。 建议使用 Azure 流量管理器 进行迁移，因为它提供了一系列的路由方法。 如何准确地更新流量传递规则取决于你要保留还是弃用现有区域，还取决于应用程序中流量的配置方式。 你可能需要调研是否可以在不同区域中的不同 Azure 资源之间移动专用/公共 IP 或 DNS 名称。 Service Fabric 不识别系统的这一部分，因此请进行调研，并在必要时让与你的流量流相关的 Azure 团队参与进来（特别是在该部分十分复杂或出现延迟对你的工作负载影响非常大的情况下）。 查看配置自定义域、公共 IP 地址和 DNS 区域和记录等文档非常有帮助。 下面是两个示例场景，演示了如何更新流量路由：

- 如果你不打算保留现有的源区域，并且有一个与网络负载均衡器（它将调用传递到原始源群集）的公共 IP 关联的 DNS/CNAME。 更新要与新区域中新的网络负载均衡器的新公共 IP 关联的 DNS/CNAME。 完成该传输将导致使用现有群集的客户端切换到使用新群集。

- 如果你打算保留现有的源区域，并且有一个与网络负载均衡器（它将调用传递到原始源群集）的公共 IP 关联的 DNS/CNAME。 设置 Azure 流量管理器的实例，然后将 DNS 名称与该 Azure 流量管理器实例相关联。 然后，Azure 流量管理器可以配置为路由到每个区域中的单个网络负载均衡器。

如果你打算保留这两个区域，则通常会进行某种类型的“反向同步”，其中事实源保留在某个远程存储中（例如 Azure SQL、Azure Cosmos DB、Blob 或文件存储），然后在区域之间进行同步。 如果这适用于你的工作负载，建议确认数据按预期在区域之间流动。

验证与测试

作为最终验证，请验证流量是否按预期流动，以及新区域（可能还有旧区域）中的应用程序是否按预期运行。可通过 Service Fabric Explorer 查看验证，参见使用 Service Fabric Explorer 可视化群集。

1. 验证新创建的 Service Fabric 集群的状态。

```
az sf cluster show `
--resource-group <NewResourceGroupName> `
--cluster-name <NewClusterName>
```

2. 检查集群运行状况，确保所有节点均正常工作。

3. 验证集群部署应用程序是否缺失。

```
az sf application list `
--resource-group <NewResourceGroupName> `
--cluster-name <NewClusterName>e"
```

4. 验证应用程序是否已部署到 Azure 目标区域的 Service Fabric 集群并正常运行。

5. 验证没有预知范围外的应用仍在访问 Azure 源区域的应用和服务。

清理资源

如果不打算保留原始源区域，此时可以删除该区域中的资源。 建议在删除资源之前等待一段时间，以防发现严重问题需要回滚到源区域。参见删除包含 Service Fabric 群集的资源组。

总结

通过以上步骤，您已经成功地将 Azure Service Fabric 集群从一个区域迁移到另一个区域。请确保在迁移过程中仔细检查每一步，以避免数据丢失或服务中断。如果遇到任何问题，可以参考 Azure 官方文档或联系 Azure 技术支持。

了解如何进行 Azure Service Fabric 集群的迁移， 相关参考文档:

- Azure Service Fabric 概述
- Azure Service Fabric 文档
- 创建 Azure Windows Service Fabric 群集
- 使用 PowerShell 部署应用程序

如有任何问题，请联系您的 Azure 支持团队。

迁移 Azure Analysis Services

要跨 Azure 区域迁移 Azure Analysis Services，请参考在区域之间移动。

如果只想迁移模型元数据而不是数据，则可以选择从 Visual Studio 部署模型。

有关更多信息：

- 了解 Analysis Services 备份和还原。
- 查阅分析服务概述。

如有任何问题，请联系您的 Azure 支持团队。

迁移 Azure Cache for Redis

本文将介绍如何将 Azure Cache for Redis 实例移动到不同 Azure 区域。

- 如果当前缓存层是高级层，则可以使用：异地复制、创建新缓存、对两个缓存执行双重写入操作、通过 RDB 文件导出和导入数据或以编程方式迁移。
- 如果当前缓存层是基本或标准层，则可以使用：创建新缓存、对两个缓存执行双重写入操作或以编程方式迁移

被动异地复制（高级）

先决条件

若要在两个缓存之间配置异地复制，必须满足以下先决条件：

- 这两个缓存是高级层缓存。
- 这两个缓存在同一 Azure 订阅中。
- 辅助链接缓存的大小等于或大于主链接缓存的大小。
- 两个缓存都已经存在并且正在运行。

准备

若要将缓存实例移到另一个区域，需要在所需的区域中创建第二个高级缓存实例。 两个缓存都运行后，可以在两个缓存实例之间设置异地复制。

异地复制不支持某些功能：

- 异地复制不支持区域冗余。
- 异地复制不支持持久性。

异地复制支持的条件：

- 如果这两个缓存都启用了群集功能并且具有相同数目的分片，则支持群集。
- 也支持不同 VNet 中的缓存，但需要注意一些问题。 有关详细信息，请参阅当缓存位于 VNet 中时是否可以使用异地复制？ 。

完成异地复制配置后，链接缓存对会有以下限制：

- 辅助链接缓存为只读。 可以从其中读取数据，但不能向其中写入任何数据。

  - 如果选择在异地主实例和异地辅助实例之间进行完全数据同步时从异地辅助实例读取数据，例如当异地主实例或异地辅助实例更新时，以及在某些重新启动的情况下，异地辅助实例会在针对它的任何 Redis 操作中引发错误，直到异地主实例和异地辅助实例之间的完全数据同步完成。
  - 应生成从异地辅助数据库读取的应用程序，以便在异地辅助数据库引发此类错误时回退到异地主数据库。
- 添加链接前辅助链接缓存中的任何数据都会被删除。 但如果以后删除了异地复制，复制的数据则会保留在辅助链接缓存中。
- 链接缓存时无法缩放任一缓存。
- 如果缓存已启用群集功能，则无法更改分片数目。
- 无法在任一缓存上启用暂存。
- 可以从任一缓存导出。
- 无法导入到辅助链接缓存。
- 只有在取消链接缓存之后，才可以删除任一链接缓存或包含它们的资源组。 有关详细信息，请参阅尝试删除链接缓存时为何操作会失败?
- 如果缓存位于不同的区域，网络传出费用将适用于在区域之间移动的数据。 有关详细信息，请参阅跨 Azure 区域复制数据的费用是多少?
- 故障转移不是自动发生的。 必须启动从主链接缓存到辅助链接缓存的故障转移。 有关如何故障转移客户端应用程序的详细信息，请参阅启动从异地主实例到异地辅助实例的故障转移。

移动

1. 若要将两个缓存链接到一起进行异地复制，请先在要用作主要链接缓存的缓存的“资源”菜单中选择“异地复制”。 接下来，在左侧的“异地复制”中选择“添加缓存复制链接”。
2. 在“兼容的缓存”列表中，选择所需辅助缓存的名称。 如果列表中未显示辅助缓存，请确认是否符合辅助缓存的异地复制先决条件。 若要按区域筛选缓存，请在地图中选择相应的区域，以便仅显示“兼容的缓存”列表中的缓存。还可以使用上下文菜单启动链接过程或查看辅助缓存的详细信息。
3. 选择“链接”将两个缓存链接在一起并开始复制过程。

具体请参阅：将 Azure Cache for Redis 实例移动到不同区

验证

可以使用左侧的“异地复制”查看复制过程的进度。还可以使用“概述”查看左侧的主缓存和辅助缓存的链接状态。复制过程完成后，“链接状态”改为“成功”。在链接过程中，主链接缓存仍然可用。 在链接过程完成之前，辅助链接缓存将不可用。

创建新的缓存（所有层）

准备

如果在移动期间不需要维护数据，则移动区域的最简单方法是在目标区域中创建新的缓存实例，并将应用程序连接到该实例。 例如，如果将 Redis 用作数据库记录的后备缓存，则可以轻松地从头开始重新生成缓存。

具体步骤，请参阅：将 Azure Cache for Redis 实例移动到不同区

注意：创建缓存需要一段时间。 可以在 Azure Cache for Redis 的“概述”页上监视进度。 如果“状态”显示为“正在运行”，则表示该缓存可供使用。

最后，将应用程序更新为使用新实例。

使用 RDB 文件导出和导入数据（高级）

开源 Redis 定义了一种标准机制，用于获取缓存的内存中数据集的快照并将其保存到文件中。 此文件名为 RDB，可由另一个 Redis 缓存读取。 Azure Cache for Redis 高级支持通过 RDB 文件将数据导入缓存实例。 可以使用 RDB 文件将数据从现有缓存传输到 Azure Cache for Redis。

注意：RDB 文件格式在 Redis 版本之间可能会更改，并且可能不会保留向后兼容性。 要从中进行导出的缓存的 Redis 版本不应高于新缓存实例的版本。

先决条件

- 这两个缓存是高级层缓存。
- 第二个缓存的缓存大小要么和原始缓存一样，要么比原始缓存大。
- 要从中进行导出的缓存的 Redis 版本不应高于新缓存实例的版本。

准备

若要将缓存实例移动到另一个区域，需要在所需区域创建第二个高级缓存实例。

移动

1. 有关如何在 Azure Cache for Redis 中导入和导出数据的详细信息， 请参阅在 Azure Cache for Redis 中导入和导出数据。

2. 更新应用程序以使用新缓存实例。

验证

可以通过关注 Azure 门户中的通知或通过查看审核日志中的事件，来监视导入操作的进度。

双重写入两个缓存（基本、标准和高级）

可以使用应用程序将数据写入到现有缓存和所设置的新缓存，而不是直接在缓存之间移动数据。 最初，应用程序首先从现有的缓存中读取数据。 当新缓存拥有必要的数据后，就可以将应用程序切换到该缓存，然后停用旧缓存。 举例来说，假设使用 Redis 作为会话存储，且应用程序会话的有效期为 7 天。 写入两个缓存一周后，即可确定新缓存包含所有未过期会话信息。 此后，可放心地依靠它，而不必担心数据丢失。

先决条件

- 第二个缓存的缓存大小要么和原始缓存一样，要么比原始缓存大。

准备

若要将缓存实例移到另一个区域，将需要在所需的区域中创建第二个缓存实例。

移动

实现此选项的一般步骤如下：

1. 修改应用程序代码以写入新实例和原始实例。
2. 继续从原始实例读取数据，直到新实例填充足够的数据为止。
3. 更新应用程序代码以仅从新实例读取和写入。

以编程方式迁移（所有层）

可以通过编程方式从现有缓存中读取数据并将其写入 Azure Cache for Redis，从而创建自定义迁移过程。 此开放源代码工具可用于将数据从一个 Azure Cache for Redis 实例复制到不同 Azure 缓存区域中的另一个实例。 还提供编译版本。 你可能还会发现，源代码可为编写自己的迁移工具提供有用指导。

先决条件

- 第二个缓存的缓存大小要么和原始缓存一样，要么比原始缓存大。

准备

- 在现有缓存所在区域中创建 VM。 如果数据集很大，请选择功能相对强大的 VM 以减少复制时间。

- 若要将缓存实例移到另一个区域，将需要在所需的区域中创建第二个缓存实例。

移动

在现有缓存所在的区域创建 VM 并在所需区域创建新缓存后，实现该选项的一般步骤是：

1. 刷新新缓存中的数据以确保其为空。 由于复制工具本身不会覆盖目标缓存中的任何现有密钥，因此需要执行此步骤。

2. 使用应用程序（例如上述开源工具）自动将数据从源缓存复制到目标缓存。 请记住，复制过程可能需要一段时间才能完成，具体取决于数据集的大小。

迁移 Azure Database for MySQL

单一服务器

Azure Database for MySQL 单一服务器计划于 2024 年 9 月 16 日之前停用。建议将 Azure Database for MySQL 单一服务器迁移到 Azure Database for MySQL 灵活服务器。

从单一服务器迁移到灵活服务器时的先决条件检查和迁移后操作

- 如果源 Azure Database for MySQL 单一服务器具有引擎版本 v8.x，请确保将源服务器的 .NET 客户端驱动程序版本升级到 8.0.32，以避免迁移到灵活服务器后出现任何编码不兼容问题。
- 如果源 Azure Database for MySQL 单一服务器的引擎版本为 v8.x，请确保在迁移之前将源服务器的 TLS 版本从 v1.0 或 v1.1 升级到 TLS v1.2，因为较旧的 TLS 版本已对灵活服务器弃用。
- 如果源 Azure Database for MySQL 单一服务器使用非默认端口（例如 3308、3309 和 3310），请将连接端口更改为 3306，因为灵活服务器不支持上述非默认端口。
- Azure Database for MySQL 灵活服务器上不支持出站规则中的服务标记 (SQL)。 在为灵活服务器配置防火墙设置时，请使用出站规则中的完全限定的域名 (FQDN)。

从单一服务器迁移到灵活服务器

了解如何从 Azure Database for MySQL 单一服务器迁移到 Azure Database for MySQL 灵活服务器。

请根据实际场景，选择相应的工具：

场景	工具	详细信息
脱机/联机	Azure Database for MySQL 导入和 Azure CLI	教程：使用 Azure CLI 的 Azure Database for MySQL Import
离线	数据库迁移服务(经典)与 Azure 门户	教程: Azure 门户与 DMS (脱机)
联机	数据库迁移服务(经典)与 Azure 门户	教程: Azure 门户与 DMS (联机)

若要详细了解如何使用其他迁移工具从单一服务器迁移到灵活服务器，请访问为迁移到 Azure Database for MySQL 选择合适的工具。

相关内容

- Azure Database for MySQL - 单一服务器的最新动态
- Azure Database for MySQL - 灵活服务器 Azure 区域

迁移 Azure Database For PostgreSQL

Azure Database for PostgreSQL - 单一服务器计划于 2025 年 3 月 28 日之前停用。 建议将 Azure Database for PostgreSQL - 单一服务器迁移到 Azure Database for PostgreSQL - 灵活服务器。

从 Azure Database for PostgreSQL - 单一服务器迁移到 Azure Database for PostgreSQL - 灵活服务器

了解如何使用单一服务器到灵活服务器迁移工具从 Azure Database for PostgreSQL - 单一服务器迁移到 Azure Database for PostgreSQL - 灵活服务器。

相关内容

- Azure Database for PostgreSQL 单一服务器的最新动态
- Azure Datbase for PostgreSQL - 灵活服务器 Azure 区域

迁移 Azure SQL 资源

将 Azure SQL 资源从一个区域移动到另一个区域，可使用 bacpac 文件进行导出和导入。

注意事项

- 为保证导出的事务处理方式一致，必须确保导出期间未发生写入活动，或者正在从数据库的事务处理方式一致性副本中导出。
- 如果是导出到 Blob 存储，则 BACPAC 文件的最大大小为 200 GB。 若要存档更大的 BACPAC 文件，请使用 SqlPackage 导出到本地存储。
- Azure 存储文件名不能以 . 结尾，并且不能包含空格字符或 <、>、*、%、&、:、\、/、? 等特殊字符。 文件名的长度应该少于 128 个字符。
- 如果导出操作超过 20 个小时，可能会取消操作。 为提高导出过程中的性能，可以进行如下操作：
    - 暂时提高计算大小。
    - 在导出期间终止所有读取和写入活动。
    - 对所有大型表上的非 null 值使用聚集索引。 如果不使用聚集索引，当时间超过 6-12 个小时时，导出可能会失败。 这是因为导出服务需要完成表格扫描，才能尝试导出整个表格。 确认表是否针对导出进行优化的一个好方法是，运行 DBCC SHOW_STATISTICS 并确保 *RANGE_HI_KEY* 不是 null 并且值分布良好。 有关详细信息，请参阅 DBCC SHOW_STATISTICS。
- 对于较大的数据库，BACPAC 导出/导入可能需要很长时间，并且可能会因各种原因失败。

BACPAC 文件导出

注意：目前不支持使用 Azure 门户从 Azure SQL 托管实例导出数据库的 BACPAC。 请参阅注意事项。

请参阅将数据库导出到 BACPAC 文件。

BACPAC 文件导入

你可以使用 .bacpac 文件将 SQL Server 数据库导入 Azure SQL 数据库或 SQL 托管实例。 可以从 Azure Blob 存储（仅限标准存储）中存储的 .bacpac 文件或从本地位置中的本地存储导入数据。 若要通过提供更多且更快的资源将导入速度最大化，请在导入过程中将数据库扩展到更高的服务层级和更大的计算大小。 然后，可以在导入成功后进行缩减。

注意：从 SqlPackage 生成的超过 4GB 的 Bacpac 文件可能无法从 Azure 门户或 Azure PowerShell 导入，并显示一条错误消息，指出 File contains corrupted data.。 这是已知问题的结果，解决方法是使用 SqlPackage 命令行实用工具导入 bacpac 文件。 有关详细信息，请参阅 SqlPackage 和 issue log。

注意：若要将数据库从 bacpac 文件迁移到 Azure SQL 托管实例中，请使用 SQL Server Management Studio 或 SQLPackage，当前不支持使用 Azure 门户或 Azure PowerShell。

请参阅从 bacpac 文件导入数据库。

验证与测试

1. **验证数据库连接**：通过 SQL 中查询数据，验证数据库连接是否正常。
2. **验证应用程序**：启动并运行依赖于 Azure SQL 的应用程序或服务，确保其正常运行。

迁移 SQL Server Stretch Database

SQL Server 2022 (16.x) 和 Azure SQL 数据库中已弃用 Stretch Database。 在数据库引擎的未来版本中将删除此功能。 请避免在新的开发工作中使用该功能，并着手修改当前还在使用该功能的应用程序。

相关内容

- Stretch Database - SQL Server Stretch Database | Microsoft Learn

迁移 Azure API 管理

如要将 API 管理实例从一个 Azure 区域移动到另一个区域，请使用该服务的备份与还原操作。 你可以使用不同的 API 管理实例名称或现有名称。

注意事项

- 在源和目标区域选择相同的 API 管理定价层。

必备条件

- 查看 API 管理备份与还原操作的要求及限制。
- 查看不备份的内容。 记录在移动实例后需要手动重新创建的设置和数据。
- 在源区域创建存储帐户。 你将使用此帐户备份源实例。

准备并移动

选项 1：使用另一个 API 管理实例名称

1. 在目标区域创建新的 API 管理实例，所用定价层与源 API 管理实例相同。 为新实例使用不同的名称。
2. 将现有 API 管理实例备份到存储帐户。
3. 将源实例的备份还原到新的 API 管理实例。
4. 如果有一个指向源区域 API 管理实例的自定义域，请更改自定义域 CNAME，使之指向新的 API 管理实例。
5. 如有不备份的内容，请手动重新创建。

选项 2：使用同一个 API 管理实例名称

注意：此选项会删除原始 API 管理实例，在迁移期间还会造成故障。 请确保在删除源实例之前进行有效备份。

1. 将现有 API 管理实例备份到存储帐户。
2. 删除源区域中的 API 管理实例。
3. 在目标区域创建新的 API 管理实例，所用名称与源区域相同。
4. 将源实例的备份还原到目标区域中的新 API 管理实例。
5. 如有不备份的内容，请手动重新创建。

验证

1. 在访问目标区域中的 API 管理实例之前，请确保成功完成还原操作。

2. 配置在还原操作过程中不会自动移动的设置。 示例：虚拟网络配置、托管标识、开发人员门户内容以及自定义域和自定义 CA 证书。
3. 访问目标区域中的 API 管理终结点。 例如，测试 API，或访问开发人员门户。

迁移 Azure 应用服务

目录

Azure 应用服务区域迁移步骤

- 先决条件
- 迁移准备
- 迁移计划
- 重定位
- 验证
- 清理

Azure Web 应用区域迁移

- 概述
- 迁移前准备
- 步骤一：备份现有 Web 应用服务
- 步骤二：创建目标区域资源
- 步骤三：部署应用服务到新区域
- 步骤四：验证部署
- 步骤五：切换流量并监控
- 步骤六：清理旧资源
- 参考文档

Auzre 应用服务区域迁移步骤

Azure 应用服务可以让你采用所选编程语言构建和托管 Web 应用、移动后端以及 RESTful API，而无需管理基础结构。 它提供自动缩放和高可用性，支持 Windows 和 Linux，并支持从 GitHub、Azure DevOps 或任何 Git 存储库进行自动部署。

应用服务资源是特定于区域的，不能跨区域移动。 必须在目标区域中创建现有应用服务资源的副本，然后将内容重定位到新应用。 如果你的源应用使用自定义域，可在完成重定位后，将其迁移到目标区域中的新应用。

先决条件

- 确保目标区域支持你要迁入的应用服务和任何相关服务。
- 验证是否有足够的权限将应用服务资源部署到目标订阅和区域。

- 验证是否为任何 Azure 策略分配了区域限制。
- 考虑任何运营成本，因为计算资源价格可能因区域而异。 若要估算可能的成本，请参阅定价计算器。

迁移准备

查明你当前正在使用的所有应用服务资源。 例如：

- 应用服务环境
- 应用服务计划
- 部署槽位
- 在 Azure 中购买的自定义域
- TLS/SSL 证书
- Azure 虚拟网络集成
- 混合连接
- 托管标识
- 备份设置

某些资源（例如导入的证书或混合连接）包含与其他 Azure 服务的集成。 有关如何跨区域移动这些资源的信息，请参阅相应服务的文档。

迁移计划

以下方面是迁移需要考虑的计划清单：

- 状态、存储和下游依赖项
- Certificates
- 配置
- VNet 连接/自定义名称/DNS
- 标识
- 服务终结点

状态、存储和下游依赖项

- 确定应用服务应用是有状态还是无状态。
- 检查应用程序代码中的内部缓存和状态。
- 禁用会话亲和性设置。在可能的情况下，建议禁用会话亲和性设置。 禁用会话亲和性可提高横向扩展的负载均衡。任何内部状态都可能会影响直接转换工作负载的规划（特别是在要求零停机时间的情况下）。在可能的情况下，重构任何应用程序状态以使应用程序无状态，为移动做准备，这可能是有益的。

- 分析数据库连接字符串。可在应用设置中找到数据库连接字符串。 但是，它们也可能在应用程序随附的配置文件中进行硬编码或管理。 在更高级别的移动工作负载规划中，分析和计划数据迁移/复制。 对于聊天式或延迟关键型应用程序，目标区域中的应用程序返回到源区域中的数据源的性能不佳。

- 分析外部缓存（例如 Redis）。应尽可能接近应用程序部署应用程序缓存。 分析缓存的填充方式、过期/逐出策略以及冷缓存在直接转换后对第一个用户访问工作负载的影响。

- 分析和计划 API（或应用程序）依赖项。

- 分析和计划区域服务。Application Insights 和 Log Analytics 数据是区域服务。 请考虑在目标区域中创建新的 Application Insights 和 Log Analytics 存储。 对于 App Insights，新资源也会影响必须作为应用配置更改的一部分进行更新的连接字符串。

Certificates

应用服务证书资源可移动到新的资源组或订阅，但不能跨区域移动。 可以导出的证书也可以导入到应用或新区域的 Key Vault 中。 此导出和导入过程等效于区域之间的移动。

配置

- 可以从 Azure 门户捕获现有应用设置和连接字符串的快照。 展开“设置”>“环境变量”，选择“应用设置”或“连接字符串”下的“高级编辑”，并保存包含现有设置或连接的 JSON 输出。 需要在新区域中重新创建这些设置，但这些值本身可能会由于连接服务中的后续区域更改而更改。

- 无法跨 Azure 地理边界导出现有 Key Vault 引用。 必须在新区域中重新创建任何必需的引用。

- 应用配置可以通过 Azure 应用程序配置或其他一些中心（下游）数据库依赖项进行管理。 查看任何应用程序配置存储区或类似的存储区，了解可能需要修改的环境和特定于区域的设置。

- 确保检查任何磁盘文件配置，该配置可能会也可能不会被应用程序设置替代。

VNet 连接/自定义名称/DNS

- 应用服务环境是 VNet 注入单租户服务。 应用服务环境网络不同于多租户应用服务，后者需要一个或两个“专用终结点”或“区域 VNet 集成”。 其他可能正在发挥作用的选项包括基于旧版 P2S VPN 的 VNet 集成和混合连接（Azure 中继服务）。

- 在目标区域中重新创建专用终结点（如使用）。 这同样适用于区域 VNet 集成。

- 应用服务环境的 DNS 通常通过客户专用自定义 DNS 解决方案进行管理（每个应用都有一个手动设置替代）。 应用服务环境为入口/出口提供负载均衡器，而应用服务本身对主机头进行筛选。 因此，可将多个自定义名称指向同一应用服务环境入口终结点。 应用服务环境不需要域验证。

标识

- 需要重新创建任何系统分配的托管标识，以及新目标区域中的应用。 通常，自动创建的 Microsoft Entra ID 应用（EasyAuth 使用的应用）默认为应用资源名称。
- 用户分配的托管标识也不能跨区域移动。 若要将用户分配的托管标识保留在应用的同一资源组中，必须在新区域中重新创建它们。
- 在重定位的服务中，向托管标识授予与要替换的原始标识相同的权限，包括组成员身份。
- 计划将标识提供者 (IDP) 重定位到目标区域。 尽管 Microsoft Entra ID 是一项全局服务，但某些解决方案依赖于本地（或下游）IDP。
- 将任何资源更新到可能依赖于 Kudu FTP 凭据的应用服务。

服务终结点

Azure 应用服务的虚拟网络服务终结点限制对指定虚拟网络的访问。 此外，还可通过这些终结点将访问限制为一系列 IPv4（Internet 协议版本 4）地址范围。 任何从外部连接到事件中心的用户都无法访问这些资源。 如果在事件中心资源的源区域中配置了服务终结点，则需要在目标区域中执行相同的操作。

若要成功将 Azure 应用服务重新创建到目标区域，必须事先创建 VNet 和子网。 如果使用 Azure 资源转移器工具执行所有这些资源的移动，则不会自动配置服务终结点。 因此，需要手动配置服务终结点，这可以通过 Azure 门户、Azure CLI 或 Azure PowerShell 来完成。

重定位

若要重定位应用服务资源，可使用 Azure 门户或基础结构即代码 (IaC)。迁移过程中源应用是可以正常访问的，在目标区域应用验证无误后，需要将流量重定位到目标区域，此过程可能出现应用无法对外提供服务的情况。

使用 Azure 门户进行重定位

使用 Azure 门户进行重定位的最大优势是其简单性。 应用、计划和内容以及许多设置将被克隆到新的应用服务资源和计划中。

使用 Azure 门户将应用服务资源重定位到新区域：

1. 创建源应用的备份。
2. 在目标区域中的新应用服务计划中创建一个应用。
3. 在目标应用中还原备份
4. 如果你使用自定义域，请使用 `asuid.`提前将其绑定到目标应用，并在目标应用中启用该域。
5. 将目标应用中的其他所有内容配置为与源应用相同，并验证你的配置。
6. 当你已准备好将自定义域指向目标应用时，重新映射域名。

使用 IaC 进行重定位

当存在现有持续集成和持续交付/部署 (CI/CD) 管道或可创建该管道时，使用 IaC。 有了 CI/CD 管道，便可通过部署操作或 Kudu zip 部署在目标区域创建应用服务资源。

验证

完成重定位后，使用推荐的准则测试和验证 Azure 应用服务：

- 将 Azure 应用服务重定位到目标区域后，运行冒烟测试和集成测试。 可手动测试或通过脚本运行测试。 确保验证所有配置和依赖资源已正确链接，以及所有已配置的数据都可访问。
- 验证所有 Azure 应用服务组件和集成。
- 对目标区域部署执行集成测试，包括所有正式回归测试。 集成测试应与适用于工作负载的业务部署和测试流程的常规节奏保持一致。
- 在某些情况下，特别是在重定位包括更新、对应用程序或 Azure 资源的更改或使用情况配置文件中的更改的情况下，使用负载测试来验证新的工作负载是否符合目的。 负载测试也是验证操作和监视覆盖范围的机会。 例如，使用负载测试来验证所需的基础结构和应用程序日志是否正确生成。 应根据已建立的工作负载性能基线来衡量负载测试。

清理

删除源应用和应用服务计划。 非免费层级中的应用服务计划会产生费用，即使其中没有正在运行的应用也是如此。

Azure Web 应用区域迁移

概述

本操作手册旨在指导如何将 Azure Web 应用（Azure Web App）从一个区域迁移到另一个区域。此过程包括备份现有应用服务、在目标区域创建新资源、部署应用服务、验证迁移结果等步骤。

迁移前准备

在开始迁移之前，请确保以下准备工作已完成：

- 已确认目标区域支持 Web 应用服务。
- 已备份所有相关数据和配置。
- 确保在迁移过程中有足够的权限进行资源创建和管理。
- 了解现有 Web 应用的依赖项和配置。

步骤一：备份现有 Web 应用

1. 登录 Azure 门户。
2. 导航到你需要迁移的 Web 应用。
3. 在左侧导航栏“设置”部分，选择“备份”。
4. 配置备份存储账户和容器，并执行备份操作。
5. 下载备份文件并安全存储。

Azure CLI 示例：

```
# 设置变量
$RESOURCE_GROUP="your-resource-group"
$APP_NAME="your-api-app-name"
$BACKUP_NAME="your-backup-name"
$CONTAINER_URL="your-storage-account-url"
# 创建备份
az webapp config backup create `
  --resource-group $RESOURCE_GROUP `
  --webapp-name $APP_NAME `
  --backup-name $BACKUP_NAME `
  --container-url $CONTAINER_URL
```

步骤二：创建目标区域 Web 应用

1. 在 Azure 门户中，导航到“创建资源”。
2. 搜索并选择“Web 应用”。
3. 填写创建 Web 应用的基本信息，并选择目标区域（即迁入区域）。
4. 配置“应用服务计划”（App Service Plan），确保选择目标区域的资源组。
5. 完成创建，并等待资源部署完成。

Azure CLI 示例：

```
# 设置变量
$TARGET_RESOURCE_GROUP="your-target-resource-group"
$TARGET_LOCATION="your-target-location"
$NEW_PLAN_NAME="your-new-app-service-plan"
$NEW_APP_NAME="your-new-api-app-name"
$SKU="your-new-sku"

# 创建资源组（如果不存在）
az group create `
  --name $TARGET_RESOURCE_GROUP `
  --location $TARGET_LOCATION
```

```
# 创建新的 App Service 计划
az appservice plan create `
  --name $NEW_PLAN_NAME `
  --resource-group $TARGET_RESOURCE_GROUP `
  --location $TARGET_LOCATION `
  --sku $SKU

# 创建新的 Web 应用
az webapp create `
  --resource-group $TARGET_RESOURCE_GROUP `
  --plan $NEW_PLAN_NAME `
  --name $NEW_APP_NAME
```

步骤三：部署应用服务到新区域

1. 导航到新创建的 Web 应用。
2. 在“设置”部分，选择“备份”。
3. 配置备份存储账户和容器，恢复备份文件到新 Web 应用。

Azure CLI 示例：

```
# 设置变量
$NEW_APP_NAME="your-new-api-app-name"
$NEW_RESOURCE_GROUP="your-new-resource-group"
$CONTAINER_URL="your-storage-account-url"
$BACKUP_NAME="your-backup-file-name"

# 恢复备份到新 Web 应用
az webapp config backup restore `
  --resource-group $NEW_RESOURCE_GROUP `
  --webapp-name $NEW_APP_NAME `
  --backup-name $BACKUP_NAME `
  --container-url $CONTAINER_URL `
  --overwrite
```

步骤四：验证部署 {步骤四验证部署-appsvc}

1. 在 Azure 门户中，导航到新区域的 Web 应用。
2. 访问 Web 应用的 URL，确保应用正常运行。
3. 检查日志和监控指标，确保没有错误或异常。

Azure CLI 示例：

```
# 设置变量
$NEW_APP_NAME="your-new-api-app-name"
$NEW_RESOURCE_GROUP="your-new-resource-group"
```

```
# 获取应用服务的 URL
az webapp show `
  --name $NEW_APP_NAME `
  --resource-group $NEW_RESOURCE_GROUP `
  --query defaultHostName `
  --output tsv
```

步骤五：切换流量并监控

1. 更新 DNS 记录或负载均衡器配置，将流量切换到新区域的 Web 应用。
2. 监控流量切换后的应用服务，确保其稳定运行。
3. 使用 Azure Monitor 和 Application Insights 进行性能和健康检查。

步骤六：清理旧资源

1. 确认新区域的 Web 应用和部署的应用服务稳定运行，并且没有问题。
2. 导航到源区域的 Web 应用。
3. 停止并删除源区域的 Web 应用服务和相关资源。
4. 删除备份文件或存储账户（如不再需要）。

Azure CLI 示例：

```
# 停止旧的 Web 应用
az webapp stop `
  --name $APP_NAME `
  --resource-group $RESOURCE_GROUP

# 删除旧的 Web 应用
az webapp delete `
  --name $APP_NAME `
  --resource-group $RESOURCE_GROUP

# 删除旧的 App Service 计划（如果没有其他应用使用）
az appservice plan delete `
  --name $PLAN_NAME `
  --resource-group $RESOURCE_GROUP
```

参考文档

- Azure 应用服务概述
- Azure 应用服务文档
- Azure 命令行接口 (CLI) 文档

如有任何问题，请联系您的 Azure 支持团队。

迁移 Azure IoT Hub

本文介绍如何将 IoT 中心迁移到新区域。

若要迁移中心，你需要一个对原始中心具有管理访问权限的订阅。 可将新的中心放到新的资源组和区域、原始中心所在的同一订阅甚至新的订阅中。 不能使用相同的名称，因为中心名称必须全局唯一。

注意事项

在迁移 IoT 中心之前，有几件事需要考虑。

- 确保原始位置中所有可用的功能在新位置中也可用。 某些服务以预览版提供，因此并非所有功能都可以在任何位置使用。
- 在创建和验证迁移的版本之前，不要删除原始资源。 一旦删除某个中心，就会将其永久删除，并且没有任何办法可以恢复，因此也就无法检查设置或数据来确保正确地复制中心。
- 原始 Azure IoT 中心的数据不会迁移。 该数据包括设备消息、云到设备 (C2D) 的命令以及作业相关的信息，例如计划和历史记录。 指标和日志记录结果也不会迁移。
- 需要针对迁移造成的停机时间做好安排。 将设备克隆到新中心需要花费一定的时间。 如果使用导入/导出方法，基准测试表明，移动 500,000 个设备可能需要大约两个小时，而移动 100 万个设备大约需要四个小时。
- 无需关闭或更改设备，即可将设备复制到新中心。
    - 如果设备最初是使用 DPS 预配的，请更新其注册以指向新的 IoT 中心。 然后，重新预配设备以更新存储在每个设备中的连接信息。
    - 否则，你必须使用导入/导出方法来移动设备，然后必须修改设备才能使用新中心。 例如，可将设备设置为使用孪生所需属性中的 IoT 中心主机名。 设备将采用该 IoT 中心主机名，请断开设备与旧中心的连接，然后将其重新连接到新中心。
- 需要更新任何证书，以便可将其用于新资源。 此外，你可能已在 DNS 表中的某个位置定义了中心，并且需要更新这些 DNS 信息。

方法

下面是我们建议的迁移 IoT 中心的常规方法。

1. 将中心及其设置导出到资源管理器模板。

2. 对模板进行所需的更改，例如，为迁移的中心更新所有地方显示的名称和位置。 对于模板中用于消息路由终结点的任何资源，请在模板中更新该资源的密钥。
3. 将模板导入到位于新位置的新资源组。 此步骤将创建新的 IoT 中心。
4. 请根据需要进行调试。
5. 添加未导出到模板中的任何内容。

   例如，使用者组就不会导出到模板中。 需要手动将使用者组添加到模板中，或者在创建中心后使用 Azure 门户来添加。
6. 将设备从原始中心复制到新中心。 此过程在管理已注册到 Azure IoT 中心的设备部分进行了介绍。

如何处理消息路由

如果你的中心使用消息路由，则导出中心模板的过程涉及路由配置，但不涉及资源本身。 如果要将 IoT 中心迁移到新区域，则必须选择是将路由资源也移动到新位置，还是将它们留在原地并继续“按原样”使用。 将消息路由到不同区域中的终结点资源可能会导致性能轻微下降。

如果中心使用消息路由，你可以采用两种做法。

- 将用于路由终结点的资源移到新位置。
  1. 在 Azure 门户中或通过资源管理器模板自己手动创建新资源。
  2. 在新位置创建的所有资源皆需进行重命名，因为它们需要具有全局唯一的名称。
  3. 在创建新中心之前，在新中心的模板中更新资源名称和资源密钥。 创建新中心时，这些资源应该存在。
- 不要移动用于路由终结点的资源。 请“在原地”使用这些资源。
  1. 在编辑模板的步骤中，需要检索每个路由资源的密钥并将其放入模板，然后再创建新中心。
  2. 中心仍引用原始路由资源，并按配置将消息路由到这些资源。 由于中心和路由终结点资源不在同一位置，因此性能会略微下降。

准备将中心迁移到另一个区域

本部分提供有关迁移中心的具体说明。

1. 将原始中心导出到资源模板，将文件保存到可以再次找到的某个位置。
2. 修改模板内容。从下载的模板文件中找到名为 `template.json` 的文件，根据实际情况，修改如下内容：

- 如果没有关联容器，请删除顶部的容器名称参数部分。
- 删除 storageEndpoints 属性。
- 将“资源”下的“位置”属性改为目标区域。

更新路由终结点资源

导出已配置路由的中心的资源管理器模板时，你会看到导出的模板中并未提供这些资源的密钥。 它们的放置由星号表示。 在导入新中心的模板并创建该中心**之前**，必须在门户中转到这些资源并检索密钥，然后填充密钥。

如果还移动了路由资源，请一并更新每个终结点的名称、ID 和资源组。

1. 检索所有路由资源所需的密钥，并将其放到模板中。 可以从 Azure 门户中的资源检索密钥。
    - 例如，如果要将消息路由到某个存储容器，请在门户中找到相应的存储帐户。 在“设置”部分下选择“访问密钥”，然后复制其中的一个密钥。 首次导出模板时，密钥如下所示：

      ```
      "connectionString": "DefaultEndpointsProtocol=https;AccountName=fabrikamstorage1234;AccountKey=****",
      "containerName": "fabrikamresults",
      ```

      检索存储帐户的帐户密钥后，请将其输入到模板上的子句 `AccountKey=****` 中，取代星号。
    - 对于服务总线队列，获取与 SharedAccessKeyName 匹配的共享访问密钥。 下面是 JSON 中的密钥和 `SharedAccessKeyName`：

      ```
      "connectionString": "Endpoint=sb://fabrikamsbnamespace1234.servicebus.chinacloudapi.cn:5671/;SharedAccessKeyName=iothubroutes_FabrikamResources;SharedAccessKey=****;EntityPath=fabrikamsbqueue1234",
      ```
    - 上述操作对于服务总线主题和 Azure 事件中心连接也适用。

通过加载模板创建新中心

使用编辑后的模板创建新中心。 若要移动路由资源，应在新位置设置资源，并更新模板中的引用，以使其匹配。 如果不移动路由资源，应将其包含在模板中并对其使用更新的密钥。

1. 登录 Azure 门户。
2. 选择“创建资源”。
3. 在搜索框中，搜索并选择“模板部署(使用自定义模板部署)”。 在模板部署屏幕上，选择“创建”。
4. 在“自定义部署”页面上，选择“在编辑器中生成自己的模板”，以便可以从文件上传模板。
5. 选择“加载文件”。

6. 浏览到已编辑的新模板并将其选中，然后选择“打开”。 随即会在编辑窗口中加载该模板。 选择“保存”。

7. 在“自定义部署”页上填写以下字段。

   订阅：选择要使用的订阅。

   资源组：选择现有资源组或创建新资源组。

   区域：如果你选择了现有的资源组，则系统会为你填充与资源组位置匹配的区域。 如果创建了新资源组，这便是该资源组所在的位置。

   连接字符串：填充中心的连接字符串。

   中心名称：为新中心命名。

8. 选择“查看 + 创建”按钮。

9. 选择“创建”按钮。 门户会验证你的模板并部署新中心。 如果有路由配置数据，该数据将包含在新中心内，但会指向位于先前位置的资源。

使用导入/导出方法将设备移动到新中心

可以使用 IoT C# 示例：适用于 C# 的 Azure IoT SDK 来进行设备的导入和导出。

具体步骤请参阅： 如何手动迁移 IoT 中心 - Azure IoT Hub

查看结果

可以在 Azure 门户中查看设备，并确认它们是否出现在新位置。

1. 使用 Azure 门户转到新中心。 选择该中心，然后选择“IoT 设备”。 你将会看到从旧中心复制到新中心的设备。 还可以查看新中心的属性。

2. 检查导入/导出错误：在 Azure 门户中转到 Azure 存储帐户，然后查看 ImportErrors.log 的 devicefiles 容器。 如果此文件为空（大小为 0），则表示未发生任何错误。 如果尝试多次导入同一设备，第二次导入时会拒绝该设备，并将一条错误消息添加到日志文件中。

提交更改

此时，你已将中心复制到新位置，并已将设备迁移到新中心。 接下来需要进行相应更改，使设备能够与新中心配合工作。

若要提交更改，需要执行以下步骤：

- 更新每个设备以更改 IoT 中心主机名，将 IoT 中心主机名指向新中心。 应使用首次预配设备时所用的相同方法执行此操作。
- 更改引用旧中心的所有应用程序，使其指向新中心。
- 完成后，新中心应会启动并运行。 旧中心应该没有活动的设备并处于断开连接状态。

回滚所做更改

如果你决定回滚更改，请执行以下步骤：

- 更新每个设备以更改 IoT 中心主机名，将 IoT 中心主机名指向旧中心。 应使用首次预配设备时所用的相同方法执行此操作。
- 更改引用新中心的所有应用程序，使其指向旧中心。 例如，如果使用的是 Azure Analytics，则可能需要重新配置 Azure 流分析输入。
- 删除新中心。
- 如果你有路由资源，则旧中心上的配置仍应指向正确的路由配置，并且在旧中心重启后，它应该仍可使用这些资源。

检查结果

若要检查结果，请将 IoT 解决方案更改为指向位于新位置的中心，然后运行它。 换而言之，请对新中心执行以前对旧中心所执行的相同操作，并确保它们正常工作。

如果已实施路由，请测试并确保将消息正确路由到资源。

清理

在确定新中心已启动并运行，并且设备可正常工作之前，请不要清理资源。 另外，如果使用了路由功能，请务必对此功能进行测试。 准备就绪后，执行以下步骤来清理旧资源：

- 删除旧中心（如果尚未这样做）。 这会从该中心删除所有活动的设备。
- 如果已将路由资源移到新位置，可以删除旧路由资源。

后续步骤

现已将 IoT 中心连同设备一起迁移到了新区域中的新中心。 有关对 IoT 中心内的标识注册表执行批量操作的详细信息，请参阅批量导入和导出 IoT 中心设备标识。

迁移 Notification Hubs

本文介绍如何将 Azure 通知中心资源移到其他 Azure 区域。 此过程大致为：

1. 创建一个使用另一名称的目标命名空间。
2. 使用导入导出方式来迁移注册。

先决条件

- 确认 Azure 订阅允许在目标区域中创建 Notification Hubs。
- Azure 通知中心命名空间名称是独一无二的，并且注册按中心进行，因此，若要执行此类移动，必须在所需区域创建新的中心，然后将注册以及所有其他相关的数据移到新创建的命名空间

创建使用其他名称的通知中心命名空间

按照以下步骤创建新的通知中心命名空间。 在**基本信息**选项卡中填写所有必需信息，包括命名空间的所需目标区域。

1. 登录 Azure 门户。
2. 在左侧菜单上选择**所有服务**，然后在 **Web + 移动**部分选择**通知中心**。在**通知中心**页面上，在工具栏上选择**创建**。
3. 在**通知中心**页面上的**基本信息**选项卡中，填写如下信息：
    - 在**命名空间详细信息**中为新命名空间输入唯一名称。
    - 命名空间包含一个或多个通知中心，因此请在**通知中心详细信息**中键入中心的名称。
    - 从**位置**下拉列表框中选择值。 此值指定要在其中创建通知中心的位置。
4. 点击创建。

创建新命名空间后，请确保设置新命名空间中的 PNS 凭据，并创建新命名空间中的等效策略。

注册迁移

- 通过导入和导出方式进行迁移，请参阅批量导出和导入 Azure 通知中心注册。

注意：导出设备信息后，需要删除设备信息中的 ExpirationTime 字段。

删除前一命名空间（可选）

完成从旧命名空间到新命名空间的注册导出后，可以根据需要删除旧命名空间。

1. 转到前一区域的现有命名空间。
2. 单击**删除**，然后在**删除命名空间**窗格中重新输入命名空间名称。
3. 单击**删除命名空间**窗格底部的**删除**。