Microsoft

由世纪互联运营的 Power BI 安全白皮书

Power BI 由世纪互联®运营

目录

引言

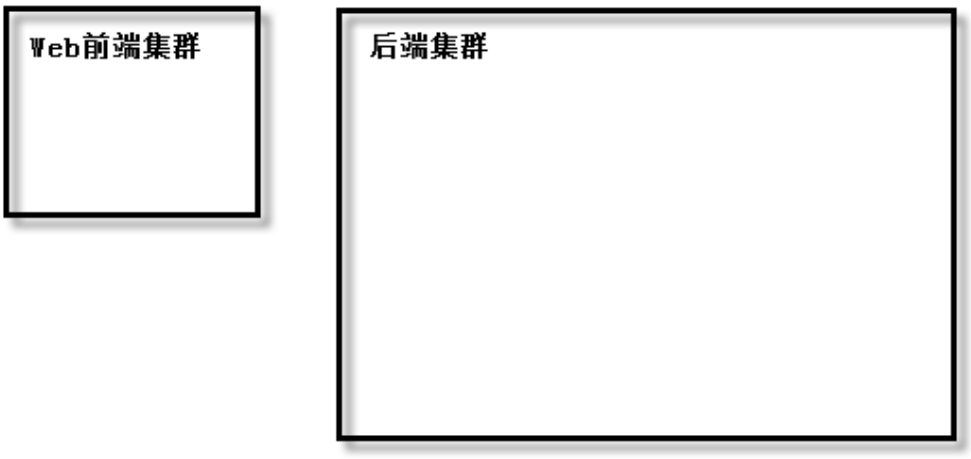
由世纪互联运营的 Power BI 是采用 Microsoft 服务于全球的技术，由北京世纪互联宽带数据中心有限公司的全资子公司上海蓝云网络科技有限公司（简称为“世纪互联”）独立运营和销售的在线软件服务（SaaS，软件即服务），可让您通过自助服务轻松快速地创建商业智能仪表盘、报表、数据集及可视化效果。借助由世纪互联运营的 Power BI，您可连接到不同的数据源，对获得的数据进行组合和构筑，然后创建可与他人共享的报表和仪表盘。

由世纪互联运营的 Power BI 服务遵循《世纪互联运营的 Office 365 在线服务标准协议》和《世纪互联运营的 Office 365 和 Power BI 隐私声明》。如需了解安全、隐私和数据保护，请参阅《世纪互联运营的Office 365在线服务标准协议》中有关安全、隐私和数据保护的规定。有关 Power BI 合规信息，请参阅信任中心。Power BI 团队致力于为客户带来最新的创意和生产力。本文描述由世纪互联运营的 Power BI 的安全性：首先介绍 Power BI 的架构，然后解释用户如何对 Power BI 进行身份验证并建立数据连接，之后说明 Power BI 如何通过服务来存储和移动数据，最后一部分是安全相关问题及解答。

由世纪互联运营的 Power BI 架构

由世纪互联运营的 Power BI 服务建立于 Microsoft Azure 之上。由世纪互联运营的 Power BI 目前部署于中国北部和东部数据中心——许多主动部署可供客户使用，同时有同等数量的被动部署处于备用状态。

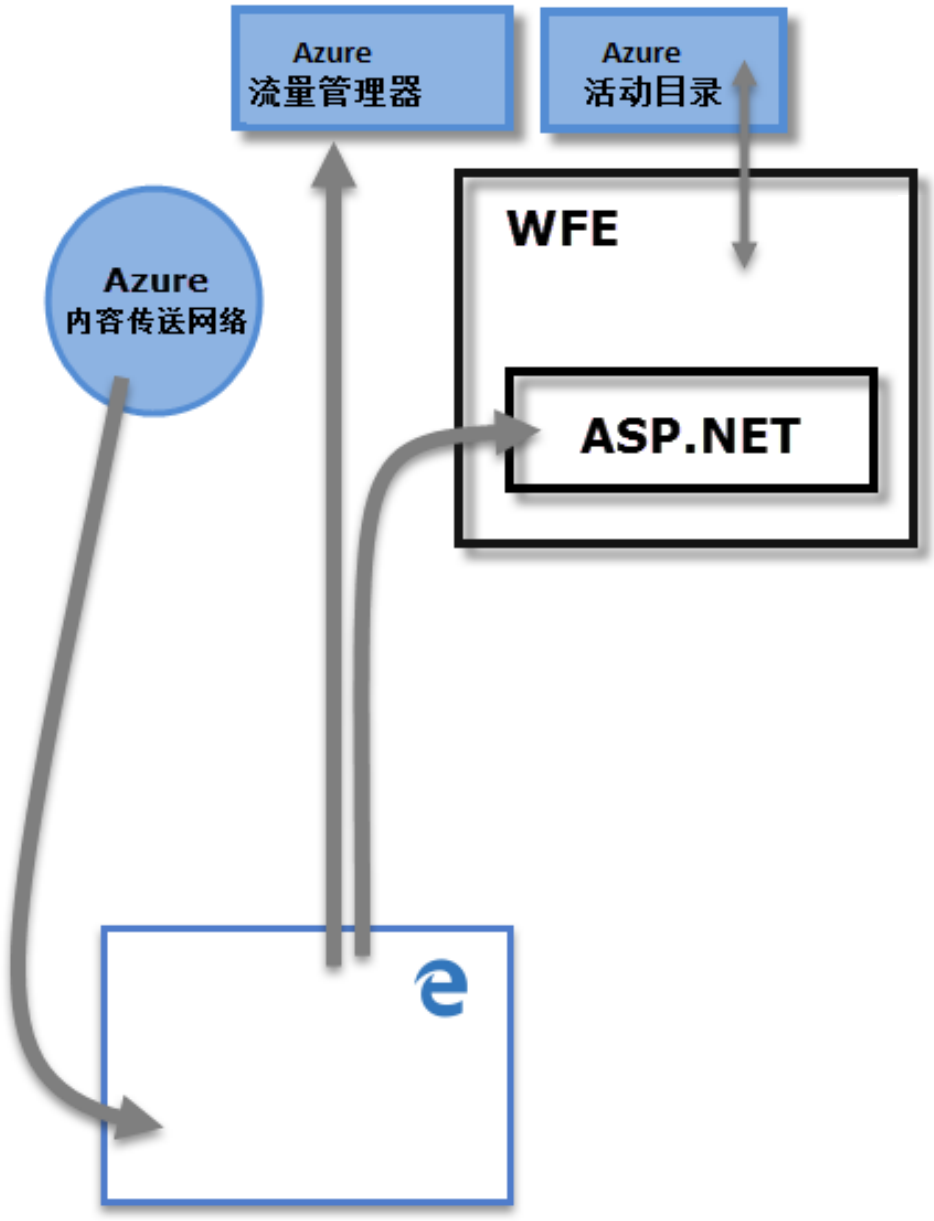
每个 Power BI 部署包含两个集群——一个 **Web 前端（WFE）**集群和一个**后端集群**。下面的图表显示了这两个集群，并为本文其他部分提供背景信息。



Power BI 使用 **Azure 活动目录（AAD）**进行账户身份验证和管理。Power BI 还使用 **Azure 流量管理器（ATM）**将用户流量引向最近的数据中心（由尝试连接的客户端的DNS记录确定），以便进行身份验证，并下载静态内容和文件。Power BI 使用 **Azure 内容传送网络 （CDN）**，可根据地理位置将必要的静态内容和文件有效地分发给用户。

WFE 集群

Web 前端（WFE）集群管理由世纪互联运营的 Power BI 的初始连接和身份验证，使用 Azure 活动目录（AAD）对客户端进行身份验证，并为后续客户端连接 Power BI 服务提供令牌。

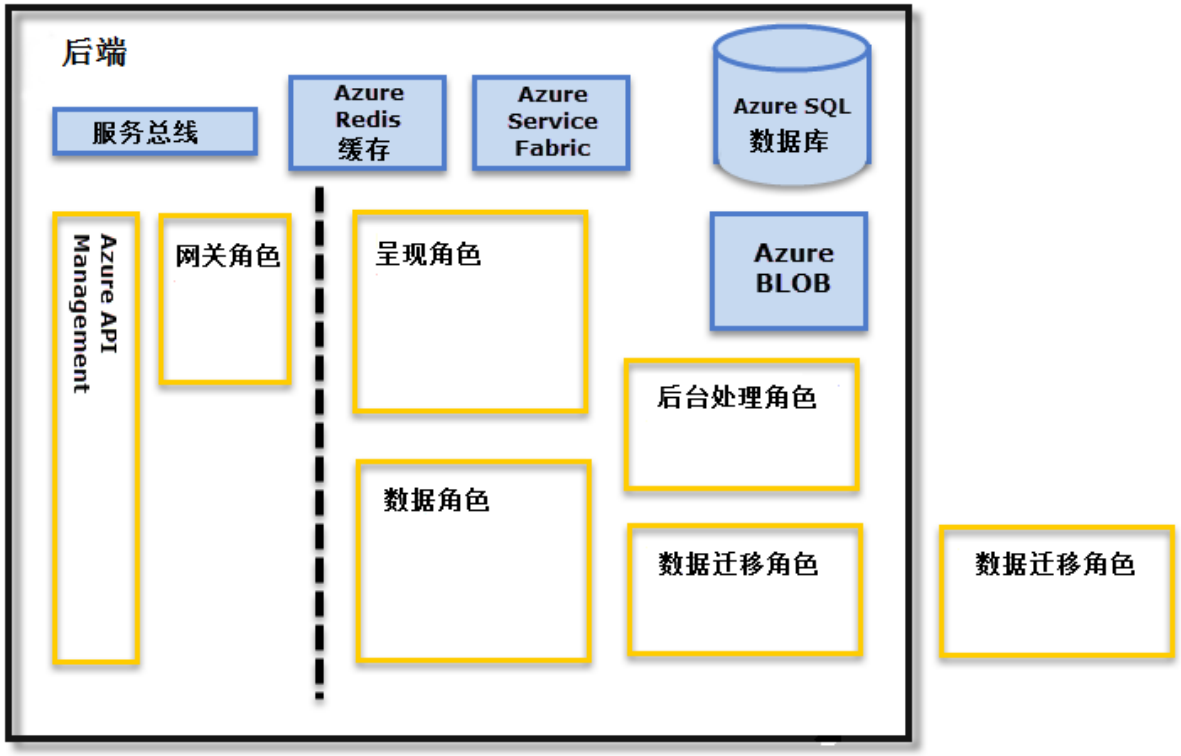


用户试图连接 Power BI 服务时，客户端的DNS服务可与 **Azure 流量管理器**进行通信，找到最近的数据中心和 Power BI 部署。如需更多信息，请浏览 Azure 流量管理器高性能流量路由办法。

距离用户最近的 Web 前端（WFE）集群负责管理登录和认证过程（后文将有介绍），一旦认证成功，将向用户提供 Azure 活动目录AAD令牌。Web 前端（WFE）群集中的ASP.NET组件将解析请求以确定用户所属的机构，然后咨询 Power BI 服务。 Power BI 服务是由世纪互联运营的 Power BI 所有 Web 前端（WFE）群集和后端集群共享的单一Azure Table，可将用户和客户机构映射到其 Power BI 租户所在的数据中心。然后 Web 前端（WFE）群集为浏览器指定可容纳该机构租户的后端集群。一旦用户通过身份验证，客户端将直接与后端集群发生交互，Web 前端（WFE）群集不再担任这些请求的中介。

由世纪互联运营的 Power BI 后端集群

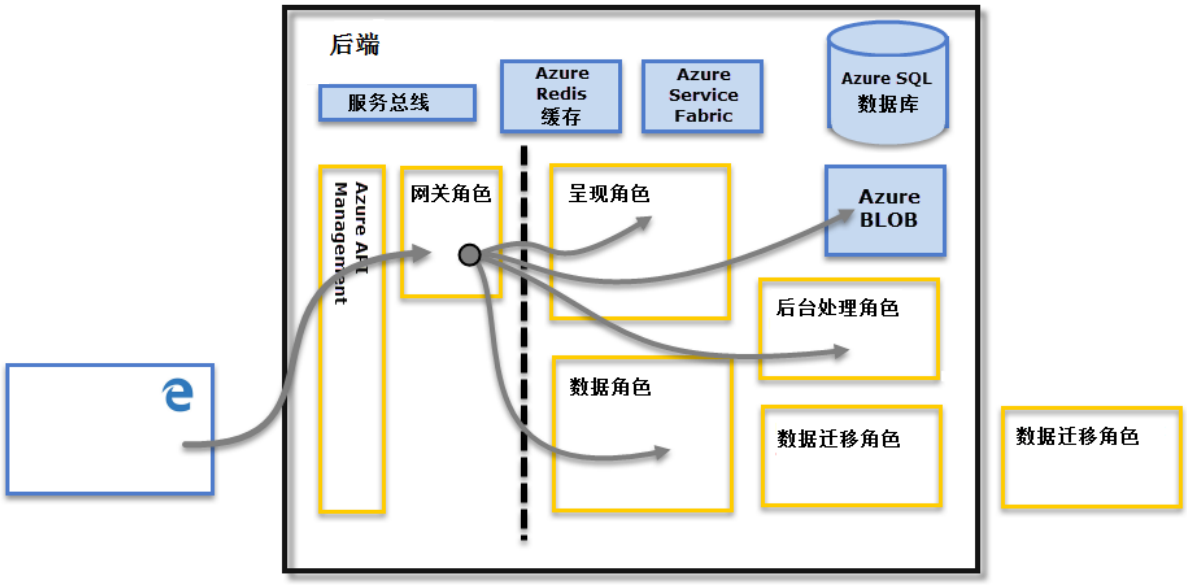
后端集群是经过验证的客户端与 Power BI 服务发生交互的方式。**后端集群**管理可视化目标、用户仪表盘、数据集、报表、数据存储、数据连接、数据刷新，以及与 Power BI 服务交互的其他方面。



网关角色（Gateway Role）是位于用户请求和 Power BI 服务之间的网关。用户不直接与网关角色以外的任何功能进行交互。**Azure API Management** 将最终处理网关角色的各项职责。

重要提示：必须注意，通过公共互联网只能访问**Azure API Management（APIM）**和**（GW）角色。**它们提供认证、授权、DDoS 保护、限流、负载平衡、路由等功能。

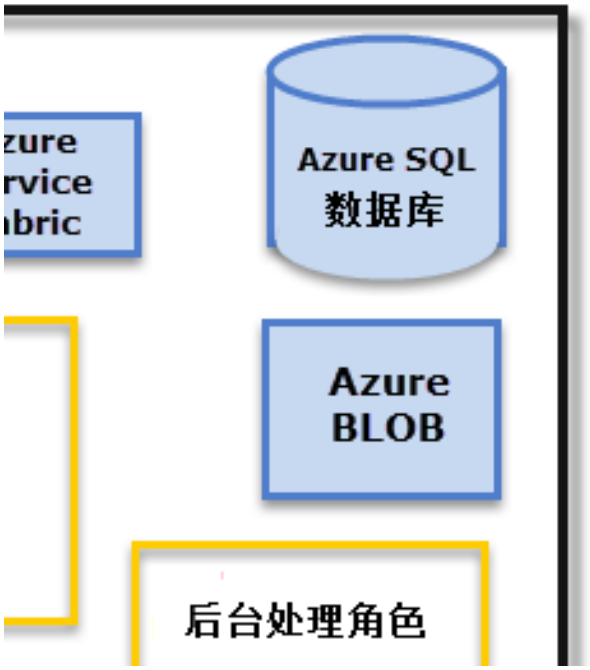
上面**后端集群**图形中的虚线划定了界限，（虚线）左侧是用户可访问的仅有的两个角色，右侧是只有系统可访问的角色。当经过身份验证的用户连接到 Power BI 服务时，客户端的连接请求和其他请求由**网关角色**和 **Azure API Management** 接收并管理，然后它们将代表用户与 Power BI 服务的其余部分进行交互。例如，当客户端尝试查看仪表盘时，**网关角色**接受该请求，然后单独向**呈现角色（Presentation Role）**发送请求，以检索浏览器呈现仪表盘所需的数据。



数据存储架构

Power BI 使用两个主存储库来存储和管理数据：用户上传的数据通常被发送到 **Azure Blob**，而系统本身的所有元数据以及工件都被存储在 **Azure SQL 数据库**中。

例如，当用户将 Excel 工作簿导入 Power BI 服务时，将创建一个内存分析服务表格数据库，然后数据将被存储在内存中，保留大约一小时（或直到系统发生内存压力）。数据同时会被发送到 **Azure Blob** 存储。



Azure SQL 数据库存储和更新有关用户订阅 Power BI 的元数据，包括仪表盘、报表、最近的数据源、工作区、组织信息、租户信息，以及其他和系统有关的元数据。储存于 Azure SQL 数据库中的所有信息都通过 Azure SQL 透明数据加密（TDE）技术被完全加密。储存在 Azure Blob 存储中的所有数据也经过加密。有关加载、存储和移动数据的更多信息，请参阅**数据存储和移动**。

租户创建

租户是 Azure 活动目录（AAD）服务的专有实例，若某一机构注册了由世纪互联运营的Microsoft 云服务（如 Azure、Power BI 或 Office 365），即可收到并拥有该项服务。各 Azure 活动目录（AAD）租户具有完全不同的特征，并独立于其他 Azure 活动目录（AAD）租户。

在最初配置 Power BI 服务时，Power BI 租户被创建于认定的最近的数据中心内。目前，Power BI 租户无法从该数据中心移动到其他位置，但 Power BI 开发团队正在研发方案，以允许租户管理员将其订购业务和数据从一个地区移动到另一个地区。

例如，如果某公司的 IT 经理决定为所有员工订购 Power BI，并且从中国北部启动了订购，那么 Power BI 将在中国北部数据中心（距离北京最近的数据中心）创建该公司的 Power BI 租户。无论其他员工居住于何处，每个员工都将连接到位于中国北部数据中心内的 Power BI 服务集群。

数据中心和地点

世纪互联仅在位于中国大陆的数据中心运营 Microsoft Azure、Office 365 和 Power BI 服务，采用微软服务于全球的技术，为客户提供全球一致的服务质量保障，且与全球其他地区由微软运营的服务在物理上和逻辑上完全独立。所有客户数据、处理这些数据的应用程序，以及承载 Microsoft Azure、Office 365 和 Power BI 服务的数据中心，全部位于中国境内。位于中国东部和中国北部的两座数据中心距离相隔 1000 公里以上，提供冗余的异地复制，为 Microsoft Azure、Office 365 和 Power BI 服务提供业务连续性支持。

在网络接入方面，由世纪互联运营的 Microsoft Azure、Office 365 和 Power BI 的数据中心通过 BGP 方式直接连接多家主流运营商（ 中国电信、中国联通、中国移动 ）的省级核心网络节点，可为用户提供高速稳定的网络访问体验。位于中国东部和北部的两个数据中心采用相同的地址广播和 BGP 路由策略，用户可以就近访问位于上述两个数据中心的服务，达到最佳网络性能体验。

两个数据中心均位于国内电信运营商的顶级数据中心，在绿色节能的基础上，采用 N+1 或者 2N 路不间断电源保护。此外还有大功率柴油发电机为数据中心提供后备电力，配有现场柴油存储和就近加油站的供油协议作为保障。数据中心机房内均设有架空地板，冷通道封闭，与后端制冷系统，冷机，冷却塔和冰池形成高效冷却循环，为机房内运行的服务器提供稳定适合的环境。数据中心配有新风系统，可在天气条件适合时最大限度地降低数据中心的 PUE 。

用户认证

由世纪互联运营的 Power BI 服务的用户身份验证包括在用户浏览器和 Power BI 服务或 Power BI 所使用的 Microsoft Azure 服务之间的一系列请求、响应和重定向。该序列描述了 Power BI 用户认证的过程。

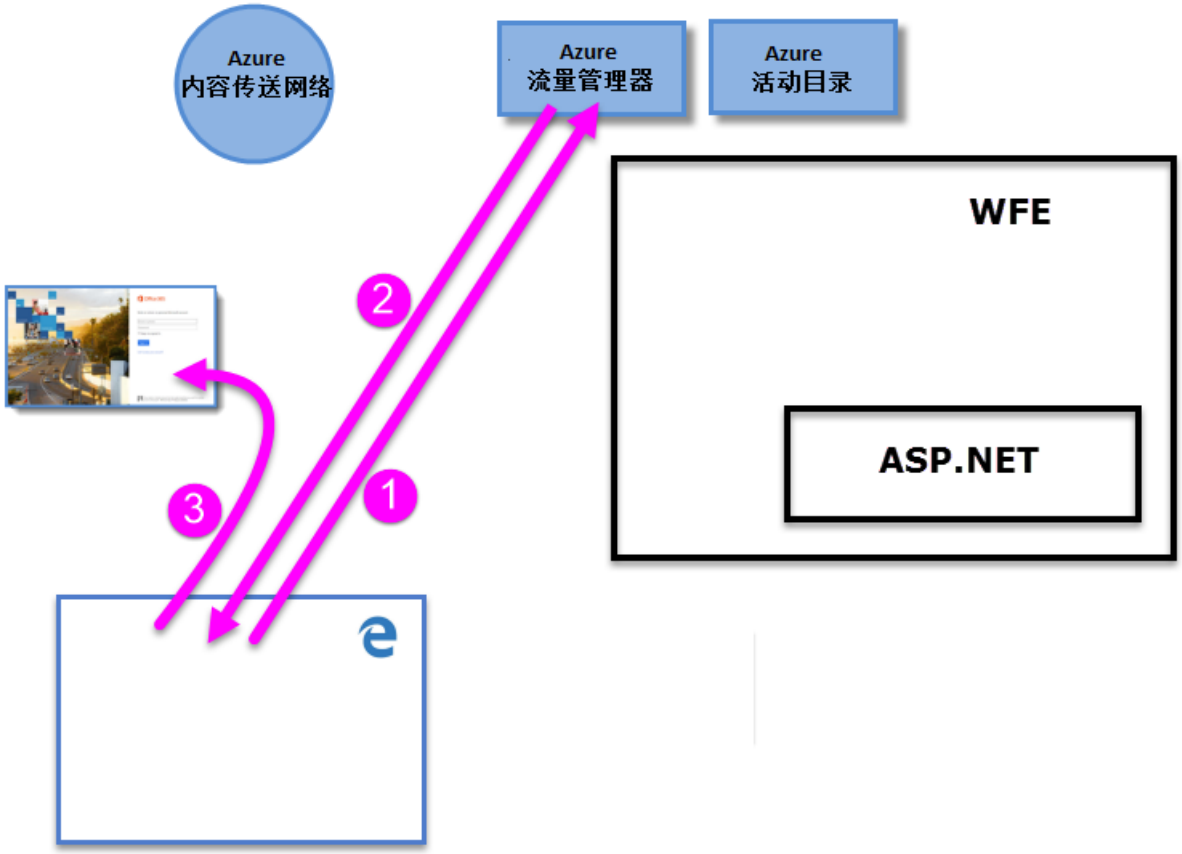
验证序列

Power BI 服务的用户认证顺序如下图所示，包括几个步骤。

1. 用户从浏览器发起与 Power BI 服务的连接，即在地址栏中输入 Power BI 地址（例如 https://app.powerbi.cn ）此连接的建立使用 TLS 1.2 和 HTTPS，而浏览器和 Power BI

服务之间的所有后续通信都使用 HTTPS。该请求被发送到 **Azure 流量管理器（Azure Traffic Manager）**。

2. **Azure 流量管理器**检查用户的 DNS 记录以确定部署有 Power BI 的最近的数据中心，并使用该用户将前往的 Web 前端（WFE）集群的 IP 地址对 DNS 进行响应。
3. Web 前端（WFE）集群然后将用户重定向到“世纪互联 Microsoft Power BI 在线服务”登录页面。

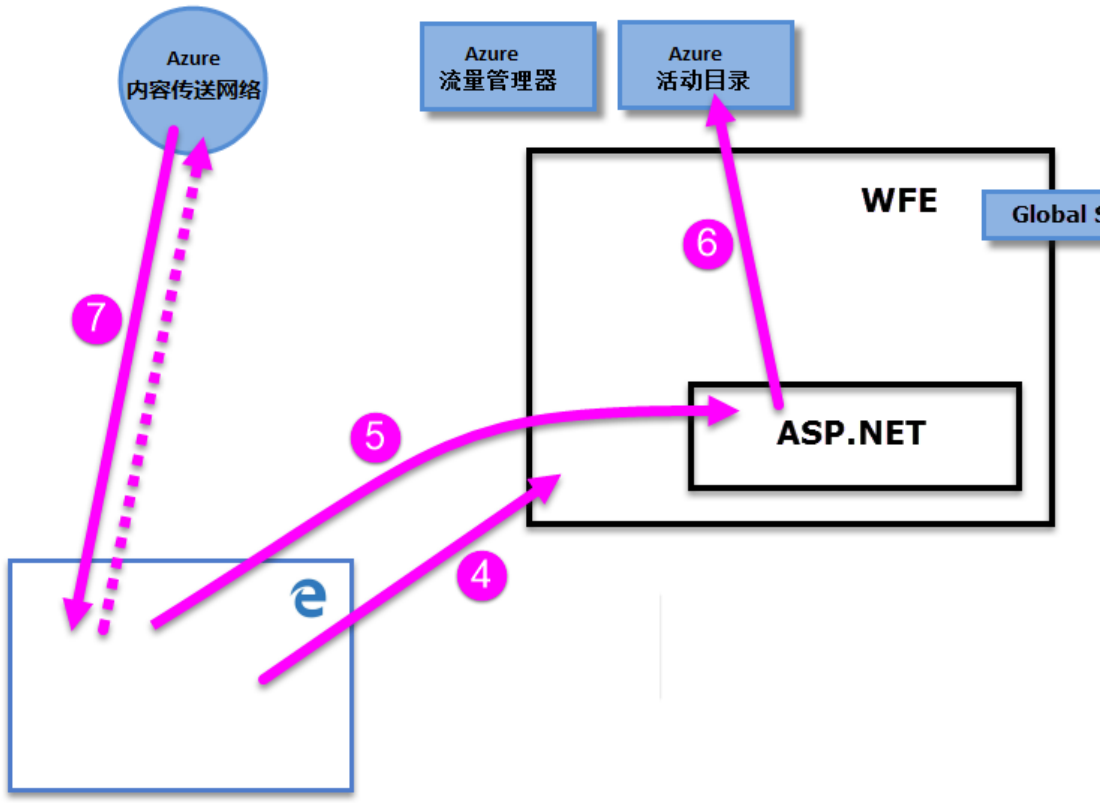


4. 一旦用户完成身份验证，登录页面将用户重定向到先前确定的最近的 Power BI 服务 Web **前端（WFE）集群**。
5. 成功登录“世纪互联在线服务”，并由 Web 前端（WFE）集群中的 **ASP.NET 服务**完成检查后，浏览器将提交获取的 cookie。

6. Web 前端（WFE）集群与 **Azure Active Directory（AAD）**服务共同实施检查，以验证用户的 Power BI 服务订购，并获取 **Azure Active Directory（AAD）**安全令牌。当 **Azure Active Directory（AAD）**将用户身份验证成功返回、并返回 **Azure Active Directory（AAD）**安全令牌时，Web 前端（WFE）集群将咨询 **Power BI 全球服务**，该服务负责维护租户及 Power BI 后端集群位置列表，并确定由哪个 Power BI 服务集群容纳该用户的租户。Web 前端（WFE）集群然后将用户引导到其租户所在的 Power BI 集群，并将一系列项目返回给用户的浏览器：

    - Azure Active Directory (AAD) 安全令牌
    - 会话信息
    - 用户可与之通信和交互的**后端集群**的 Web 地址

7. 用户浏览器然后联系指定的 Azure CDN 或（对某些文件）Web 前端（WFE）集群，下载指定的通用文件集合，以便浏览器与 Power BI 服务进行交互。在 Power BI 服务浏览器会话期间，浏览器页面包括 Azure 活动目录（AAD）令牌、会话信息、关联的后端集群的位置，以及从 Azure CDN 和 Web 前端（WFE）集群下载的文件集合。



一旦完成这些项目，浏览器将启动与指定后端集群的联系，用户与 Power BI 服务的交互即开始。从此点开始，所有对 Power BI 服务的调用都使用指定的后端集群，所有呼叫都包含用户的 Azure 活动目录（AAD）令牌。

数据存储和移动

在由世纪互联运营的 Power BI 服务中，数据或者处于静止状态（Power BI 用户可获得的、当前未被处理的数据），或者处于*正在处理状态*（例如：正在运行的查询、正在处理的数据连接和模型、正上传到 Power BI 服务的数据和/或模型，以及用户或 Power BI 服务可对主动访问或更新的数据采取的其他操作）。正在被处理的数据被称为*处理中数据*。Power BI 中的静态数据经过加密处理。正在传输的数据，即 Power BI 服务发送或接收的数据也经过加密。

由世纪互联运营的 Power BI 服务还根据是否使用 DirectQuery 访问数据来对数据实施不同的管理。因此，Power BI 有两类用户数据：DirectQuery 访问的数据和 DirectQuery 不能访问的数据。

DirectQuery 是一种经过转化的查询，表示 Power BI 用户的查询已经从 Microsoft 的数据分析表达式（DAX）语言（Power BI 和其他 Microsoft 产品创建查询所使用的语言）转化为数据源的本机数据语言（如 T-SQL 或其他本地数据库语言）。与 DirectQuery 相关联的数据仅通过引用被存储下来，这表示当 DirectQuery 不活动时，源数据不会存储在由世纪互联运营的 Power BI 中（除了用于显示仪表盘和报表的可视化数据，参见下文*处理中数据（数据移动）*）。同时，引用的 DirectQuery 数据被存储下来，以便在运行 DirectQuery 时访问该数据。DirectQuery 包含执行查询所需的所有必要信息，包括用于访问数据源的连接字符串和凭据，以便 DirectQuery 连接到内含数据源进行自动刷新。使用 DirectQuery 时，基础数据模型信息被并入DirectQuery。

未使用DirectQuery 的查询包含一组 DAX 查询，这些查询不直接转换为任何基础数据源的本机语言。非 DirectQuery 查询不包括基础数据凭据，基础数据将被加载到由世纪互联运营的 Power BI 服务。

DirectQuery 和其他查询之间的区别决定了由世纪互联运营的 Power BI 服务如何处理静态数据，以及查询本身是否被加密。以下部分介绍静态数据和移动数据，并解释加密、位置和数据处理流程。

静态数据

当数据处于静止状态时，由世纪互联运营的 Power BI 服务将按照下述方式存储数据集、报表和仪表盘。如前所述，由世纪互联运营的 Power BI 中的静态数据经过加密处理。下文中，ETL 表示“提取、转换和加载”。

加密密钥

- Azure Blob 密钥的加密密钥被加密存储于 Power BI 服务的单独位置。
- Azure SQL 数据库透明数据加密(TDE)技术的加密密钥由 Azure SQL 自身管理。
- “数据移动”服务的加密密钥存储于：
    - “数据移动角色”（Data Movement Role）——基于云的数据源

用于加密 Windows Azure Blob 存储的“内容加密密钥”（CEK）是随机生成的 256 位密钥。CEK 用于加密内容的算法是 AES_CBC_256。

用于加密 CEK 的“密钥加密密钥”（KEK）是预定义的 256 位密钥。KEK 加密 CEK 的算法是 A256KW。

基于恢复密钥的加密密钥从不离开本地基础设施。由世纪互联运营的 Power BI 无法访问加密的本地凭据值，并且无法拦截这些凭据；Web 客户端使用与其正在通信的特定网关相关联的公钥来加密凭据。

对于基于云的数据源，“数据移动角色”（Data Movement Role）使用始终加密方法对加密密钥进行加密。您可浏览始终加密数据库功能了解更多信息。

数据集

1. 元数据（表格、列、度量、计算、连接字符串等）
    a. 对于本地分析服务（Analysis Service）来说，若非引用在 Azure SQL 中加密的数据库，服务中不存储任何内容。
    b. ETL、DirectQuery 和 Push Data（推送数据）的所有其他元数据都被加密存储于 Azure Blob 存储。

2. 原始数据源凭据
    a. 本地分析服务——无需凭据，因此不存储任何凭据。
    b. DirectQuery——取决于是否直接在服务中创建模型，若是，将被存储于连接字符串中并在 Azure Blob 中被加密；若需从 Power BI Desktop 中导入模型，凭据将在“数据移动”（Data Movement）的 Azure SQL 数据库中被加密存储。
    c. 推送数据——不适用
    d. ETL
        - 对于 **Salesforce** 或 **OneDrive——**刷新令牌将被加密存储在 Power BI 服务的 Azure SQL 数据库中。
        - 其他情况：
            - 如果数据集被设置为刷新，凭据将被加密存储在“数据移动”（Data Movement）的 Azure SQL 数据库中。
            - 如果数据集未被设置为刷新，则不会为数据源存储凭据

3. 数据
    a. 本地分析服务和 DirectQuery ——Power BI 服务中不存储任何内容。
    b. ETL——在 Azure Blob 存储中加密。
    c. 推送数据 v1——在 Azure Blob 存储中被加密存储。
    d. 推送数据 v2——在 Azure SQL 中被加密存储。

由世纪互联运营的 Power BI 采用客户端加密方法，以带有高级加密标准（AES）的密码块链接（CBC）模式来加密 Azure Blob 存储。您可在此了解有关客户端加密的更多信息。
由世纪互联运营的 Power BI 通过以下方式提供数据完整性监控：

- 对 Azure SQL 中的静态数据，Power BI 使用 dbcc、TDE 和常量页校验和（作为 SQL 本地产品的一部分）。

- 对 Azure Blob 存储中的静态数据，Power BI 使用客户端加密和 HTTPS 将数据传输到存储器，其中包括检索数据期间的完整性检查。您可在此了解有关 Azure Blob 存储安全性的更多信息。

报表

1. 元数据（报表定义）
    a. 报表可以是 Excel for Office 365 报表，也可以是 Power BI 报表。以下叙述适用于基于报表类型的元数据：

a. Excel 报表元数据经加密存储于 SQL Azure。元数据也存储于 Office 365 中。

b. Power BI 报表被加密存储于 Azure SQL 数据库。

2. 静态数据

   静态数据包括背景图像和自定义视觉效果等工件。

   a. 对于使用 Excel for Office 365 创建的报表，不存储任何内容。

   b. 对于 Power BI 报表，静态数据将被加密存储于 Azure Blob 存储中。

3. 缓存

   a. 对于使用 Excel for Office 365 创建的报表，不缓存任何内容。

   b. 对于 Power BI 报表，视觉效果数据经过加密被缓存在 Azure SQL 数据库中。

4. 发布到 Power BI 的原始 Power BI Desktop（.pbix）或 Excel（.xlsx）文件

   .xlsx 或.pbix 文件的副本或影子副本有时被存储于 Power BI 的 Azure Blob 存储中，此时数据将被加密。

仪表盘和仪表盘板块

1. 缓存——仪表盘上的视觉效果需要的数据通常被缓存并加密存储于 Azure SQL 数据库中。来自 Excel 或“SQL 服务器报告服务”（SSRS）的固定视觉效果等板块，作为图像被存储于 Azure Blob 中，同时经过加密。
2. 静态数据——包括加密存储于 Azure Blob 存储中的工件，如背景图像和自定义视觉效果。

暂时存储在非易失性设备上的数据

下文介绍暂时存储在非易失性设备上的数据。

数据集

1. 元数据（表格、列、度量、计算、连接字符串等）
2. 某些与模式相关的工件可在有限的时间内被存储于计算节点的磁盘上。某些工件也可存储于 Azure REDIS 缓存中，在有限的时间内未经加密。

3. 原始数据源凭据
    a. 本地分析服务——不存储任何内容
    b. DirectQuery——取决于是否直接在服务中创建模型，若是，将以加密形式存储于连接字符串中，同时加密密钥以明文存储在一起（在加密信息旁边）；若需从 Power BI Desktop 中导入模型，凭据将不会被存储在非易失性设备上。
    c. 推送数据——无（不适用）
    d. ETL——无（计算节点上不存储任何内容，与上文“**静态数据**”所示相同）

4. 数据
    某些数据工件可在有限的时间内被存储于计算节点的磁盘上。

处理中数据

当用户主动使用或访问数据时，数据处于正在处理状态。例如，当用户访问数据集、修改或修订仪表盘或报表、进行刷新时，或发生其他数据访问活动时，数据处于正在处理中。当这些事件发生并将数据置于处理状态时，由世纪互联运营的 Power BI 服务中的数据角色（Data Role ）将创建内存分析服务（AS）数据库，并将数据集加载到该内存分析服务数据库。无论数据集是否基于 DirectQuery，加载到 AS 数据库中的数据都未经加密以允许数据角色的访问，并被保存于内存中方便进一步访问，直到由世纪互联运营的 Power BI 服务不再需要该数据集。

一旦数据被处理，包括初始加载数据到由世纪互联运营的 Power BI 中，由世纪互联运营的 Power BI 服务即将可视化数据缓存在加密的 Azure SQL 数据库中，不考虑数据集是否基于 DirectQuery。

为监控正在处理的数据的数据完整性，由世纪互联运营的 Power BI 使用 HTTPS、TCP/IP 和 TLS 来确保数据被加密，并在传输过程中保持完整性。

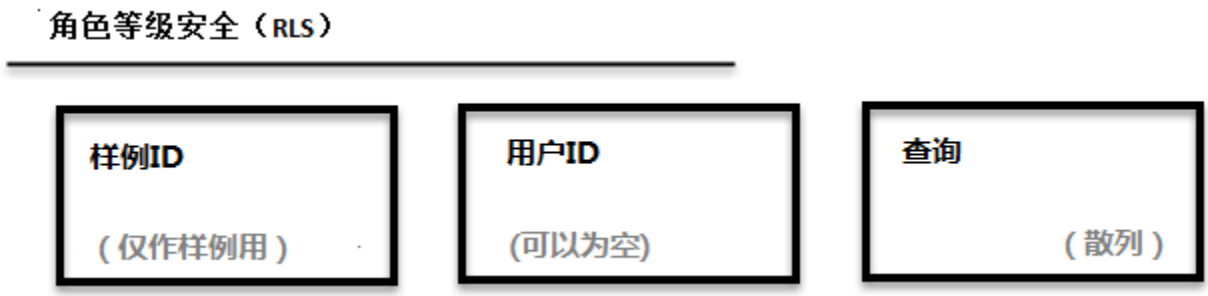
用户对数据源的身份验证

用户根据自身登录情况与各个数据源建立连接，并使用这些凭据访问数据。之后用户可根据基础数据创建查询、仪表盘和报表。

当用户分享查询、仪表盘、报表或任何可视化效果时，对该数据和可视化效果的访问取决于基础数据源是否支持角色等级安全（RLS）。

如果基础数据源能够支持由世纪互联运营的 **Power BI 的角色等级安全（RLS）**，则 Power BI 服务将应用该角色等级安全，没有足够凭据访问基础数据的用户（可能是用于仪表盘、报表或其他数据工件的查询）将无法看到其没有足够凭据浏览的数据。如果访问基础数据的用户与创建仪表盘或报表的用户不同，则可视化效果和其他工件将仅显示符合用户数据访问级别的数据。

如果数据源不支持 RLS，则由世纪互联运营的 Power BI 登录凭据将被应用于基础数据源，或者如果在连接期间提供了其他凭据，则将应用这些新提供的凭据。当用户从非 RLS 数据源将数据加载到由世纪互联运营的 Power BI 服务中时，数据将按照本文档**数据存储和移动**部分的规定被存储于由世纪互联运营的 Power BI 中。对于非 RLS 数据源，当数据被分享给其他用户（例如通过仪表盘或报表）或被刷新时，原始凭据被用于访问或显示数据。



这里简单举例对比 RLS 和非 RLS 数据源，A 创建了一个报表和一个仪表盘，然后将它们分享给客户 B 和客户 C。如果报告和仪表盘使用的数据源来自不支持 RLS 的数据源，那么客户 B 和客户 C 都能够看到 A 在仪表盘中使用的数据（已上传到由世纪互联运营的 Power BI 服务），同时客户 B 和客户 C 可以与数据进行交互。相比之下，如果 A 从支持 RLS 的数据源创建了报告和仪表盘，然后与客户 B 和客户 C 共享，当客户 B 尝试查看仪表盘时，将发生以下情况：

1. 由于仪表盘使用了 RLS 数据源，仪表盘的可视化效果将简要显示“加载”消息，而由世纪互联运营的 Power BI 服务将查询数据源以检索与仪表盘底层查询相关联的连接字符串中指定的当前数据集。

2. 对数据的访问和检索将基于户 B 的凭据和角色，只有当户 B 具有足够授权时，数据才会被加载到仪表盘和报表中。
3. 能否显示仪表盘和报表中的可视化信息也基于户 B 的角色级别。

如果要访问共享的仪表盘或报表，基于他的角色级别，将发生同样的序列事件。

由世纪互联运营的 Power BI 和 ExpressRoute

通过由世纪互联运营的 Power BI 和 ExpressRoute，您可创建从您的机构到由世纪互联运营的 Power BI 的专用网络连接（或使用 ISP 的托管设施），从而绕过互联网、更好地保护敏感的 Power BI 数据和连接。

ExpressRoute 是一种 Azure 服务，可让您在 Azure 数据中心（Power BI 所在位置）和本地基础设施之间创建私人连接，或者在 Azure 数据中心和您的托管环境之间建立私人连接。如需更多信息，请参阅 Power BI 和 ExpressRoute。

Power BI Mobile

Power BI Mobile 是为三大移动平台设计的应用程序集合：Android、iOS 和 Windows Mobile。Power BI Mobile 应用程序的安全注意事项分为两类：

- 设备通信
- 设备上的应用程序和数据

就**设备通信**，所有 Power BI Mobile 应用程序可与 Power BI 服务进行通信，并使用浏览器使用的相同连接和身份验证顺序，本白皮书前文对此有详细介绍。iOS 和 Android Power BI 移动应用程序将在应用程序本身中启动浏览器会话，Windows 移动应用程序则会启动代理程序与 Power BI 建立通信通道。

Power BI Mobile 应用程序主动与 Power BI 服务进行通信。遥测用于收集移动应用使用统计数据和类似信息，将其传输到监控使用和活动的服务；未使用遥测数据发送个人身份信息（PII）。

设备上的 Power BI 应用程序会在设备上存储数据以方便使用应用程序：

- Azure Active Directory 和刷新令牌以行业标准安全措施被存储于设备的安全机制中。
- 数据被缓存在设备的存储中，未被应用程序本身直接加密。
- 设置也未经加密被存储于设备上，但不存储实际的用户数据。

Power BI Mobile 应用程序不会查看设备上的文件夹。您可在此了解有关 Power BI Mobile 应用程序离线数据的更多信息。

由世纪互联运营的 Power BI 安全问题和解答

以下是常见的由世纪互联运营的 Power BI 安全问题和答案。

1. 使用由世纪互联运营的 Power BI 时，用户如何连接并访问数据源？

由世纪互联运营的 Power BI 凭据和域凭据：用户使用电子邮件地址登录 Power BI；当用户尝试连接数据资源时，Power BI 会将 Power BI 登录电子邮件地址作为凭据进行传递。对于域连接资源（本地或基于云），登录电子邮件将与目录服务的*用户主体名称*进行匹配，以确定是否有足够凭据允许访问。对于使用工作电子邮件地址登录 Power BI 的机构（使用相同的电子邮件登录工作资源，例如 *david@contoso.com*），映射可无缝发生；对于不使用工作电子邮件地址（如 david@contoso.onmicrosoft.com）的机构，则必须建立目录映射，以便通过 Power BI 登录凭据访问本地资源。

非域连接：对于非域连接、且不支持角色等级安全（RLS）的数据连接，用户必须在连接期间提供凭据，然后由世纪互联运营的 Power BI 将凭据传递给数据源以建立连接。如果有足够权限，数据将从数据源加载到由世纪互联运营的 Power BI 服务。

2. 数据如何传输到由世纪互联运营的 Power BI？

由世纪互联运营的 Power BI 请求和发送的所有数据都经过加密传输，并使用 HTTPS 从数据源连接到由世纪互联运营的 Power BI 服务。将与数据提供商建立安全连接，只有在建立安全连接后，数据才能通行网络。

3. 由世纪互联运营的 Power BI 如何缓存报表、仪表盘或模型数据？安全吗？

访问数据源时，Power BI 服务遵循上文**数据存储和移动**规定的程序。

4. 客户端是否在本地缓存网页数据？

当浏览器客户端访问由世纪互联运营的 Power BI 时，Power BI 网络服务器将*缓存控制*（*Cache-Control*）指令设置为*不存储*（*no-store*）。*不存储*指令指示浏览器不缓存用户正在查看的网页，而且不将网页存储在客户端的缓存文件夹中。

5. 基于角色的安全性、共享报表或仪表盘、以及数据连接，这些方面安全性如何？在数据访问、仪表盘查看、报表访问或刷新方面如何保证安全？

对于**未启用角色等级安全（RLS）**的数据源，如果仪表盘、报表或数据模型通过 Power BI 被分享给与其他用户，则该数据可供共享用户查看和交互。由世纪互联运营的 Power BI 不会根据数据的原始来源重新验证用户身份；数据一旦上传到 Power BI 中，经过源数据身份验证的用户将负责管理哪些用户和群组可以查看数据。

对支持 **RLS** 的数据源（如分析服务数据源）进行数据连接时，由世纪互联运营的 Power BI 仅缓存仪表盘数据。若由世纪互联运营的 Power BI 使用的数据来自支持 RLS 的数据源，每次查看或访问报表或数据集时，Power BI 服务将根据用户凭据访问数据源以获取数据，如果权限足够，则数据被加载到该用户的报表或数据模型中。如果身份验证失败，用户将看到错误显示。

如需更多信息，请参阅上文**用户对数据源的身份验证**。

6. 由世纪互联运营的 Power BI 组如何工作？

由世纪互联运营的 Power BI 组允许用户在已建立的团队中，以快速轻松的方式协作创建仪表盘、报表和数据模型。例如，如果您有一个 Power BI 组，其中包括您直接团队中的每个成员，您即可在由世纪互联运营的 Power BI 中选择组来与团队中的每个人轻松协作。由世纪互联运营的 Power BI 组相当于 Office 365 通用组，使用与 Azure 活动目录相同的身份验证机制来保护数据。 您可在 Power BI 中创建组或在 Office 365 管理中心中创建通用组；两种方式在 Power BI 中具有同样的的组创建效果。

注意，由世纪互联运营的 Power BI 组共享数据与由世纪互联运营的 Power BI 中的任何共享数据一样，遵循同样的安全考虑。对不支持 RLS 的数据来源，Power BI 不会根据数据的原始来源重新验证用户身份；数据一旦上传到由世纪互联运营的 Power BI 中，经过源数据身份验证的用户将负责管理哪些用户和群组可以查看数据。如需更多信息，请参阅上文**用户对数据源的身份验证**。

您可浏览 Power BI 官网了解更多信息。

结论

由世纪互联运营的 Power BI 服务架构基于两个集群——一个 Web 前端（WFE）集群和一个后端集群。WFE 集群负责由世纪互联运营的 Power BI 服务的初始连接和身份验证，一旦经过身份验证，后端将处理所有后续的用户交互。由世纪互联运营的 Power BI 使用 Azure 活动目录（AAD）来存储和管理用户身份，并分别使用 Azure Blob 和 Azure SQL 数据库来管理数据和元数据的存储。

根据是否使用 DirectQuery 访问数据，Power BI 对数据存储和数据处理采用不同的方式，这取决于数据源在云中还是在本地。Power BI 还能够实施角色等级安全（RLS），并与提供本地数据访问的网关进行交互。

其他资源

如需了解有关 Power BI 的其他信息，请参阅下述资源。

- Power BI 官网
- 开始使用 Power BI Desktop