# 保护对 DocumentDB 数据的访问

本文概述了保护对存储在 [Microsoft Azure DocumentDB](https://azure.microsoft.com/services/documentdb/) 中的数据的访问。

阅读本概述后，你将能够回答以下问题：

* 什么是 DocumentDB 主密钥？
* 什么是 DocumentDB 只读密钥？
* 什么是 DocumentDB 资源令牌？
* 如何使用 DocumentDB 用户和权限来保护对 DocumentDB 数据的访问？

## DocumentDB 访问控制概念

DocumentDB 提供一流的概念，以便控制对 DocumentDB 资源的访问。在本主题中，DocumentDB 资源分为两类：

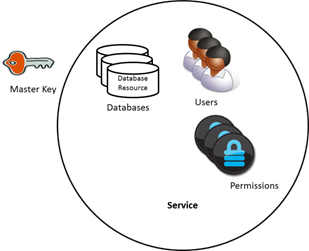
* 管理资源
  + 帐户
  + 数据库
  + 用户
  + 权限
* 应用程序资源
  + 集合
  + 文档
  + 附件
  + 存储过程
  + 触发器
  + 用户定义的函数

在这两个类别的上下文中，DocumentDB 支持三种类型的访问控制角色：帐户管理员、只读管理员和数据库用户。每个访问控制角色的权限为：

* 帐户管理员：对给定的 DocumentDB 帐户中的所有资源（管理和应用程序）的完全访问权限。
* 只读管理员：对给定的 DocumentDB 帐户中的所有资源（管理和应用程序）的只读访问权限。
* 数据库用户：与一组特定的 DocumentDB 数据库资源（如集合、文档、脚本）关联的 DocumentDB 用户资源。可以有一个或多个用户资源与给定的数据库关联，并且每个用户资源可能具有一个或多个与其关联的权限。

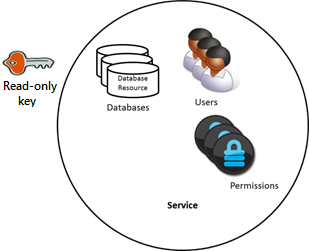
使用前面提到的类别和相关资源，DocumentDB 访问控制模型定义了三种类型的访问构造：

* 主密钥：创建 DocumentDB 帐户时，将创建两个主密钥（主要和辅助）。这些密钥可实现对 DocumentDB 帐户中所有资源的完全管理访问权限。



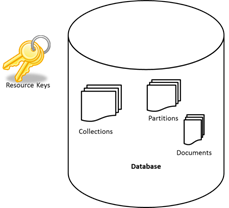
DocumentDB 主密钥插图

* 只读密钥：创建 DocumentDB 帐户时，将创建两个只读密钥（主要和辅助）。这些密钥可实现对 DocumentDB 帐户中所有资源的只读访问权限。



DocumentDB 只读密钥插图

* 资源令牌：资源令牌与 DocumentDB 权限资源关联，可捕获数据库用户与该用户对某个特定 DocumentDB 应用程序资源（如集合、文档）的权限之间的关系。



DocumentDB 资源令牌插图

## 使用 DocumentDB 主密钥和只读密钥

前面曾提到，DocumentDB 主密钥提供对 DocumentDB 帐户中所有资源的完全管理访问权限，而只读密钥实现对该帐户中所有资源的只读访问权限。下面的代码片段说明了如何使用 DocumentDB 帐户终结点和主密钥来实例化 DocumentClient 并创建新的数据库。

//Read the DocumentDB endpointUrl and authorization keys from config.  
//These values are available from the Azure Classic Portal on the DocumentDB Account Blade under "Keys".  
//NB > Keep these values in a safe and secure location. Together they provide Administrative access to your DocDB account.  
  
private static readonly string endpointUrl = ConfigurationManager.AppSettings["EndPointUrl"];  
private static readonly SecureString authorizationKey = ToSecureString(ConfigurationManager.AppSettings["AuthorizationKey"]);  
   
client = new DocumentClient(new Uri(endpointUrl), authorizationKey);  
  
// Create Database  
Database database = await client.CreateDatabaseAsync(  
 new Database  
 {  
 Id = databaseName  
 });

## DocumentDB 资源令牌概述

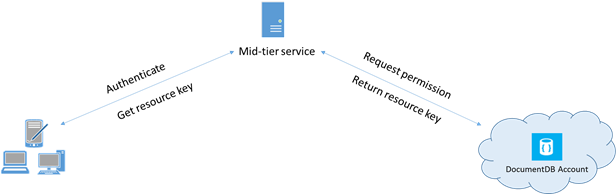
如果想要为不能通过主密钥得到信任的客户端提供对 DocumentDB 帐户中资源的访问权限，你可以使用资源令牌（通过创建 DocumentDB 用户和权限）。你的 DocumentDB 主密钥包括主要密钥和辅助密钥，这两种密钥都授予对你的帐户以及其中所有资源的管理访问权限。公开这两种主密钥的任何一种都会向可能的恶意或负面使用开放你的帐户。

同样，DocumentDB 只读密钥提供对 DocumentDB 帐户中所有资源的读取访问权限，当然权限资源除外，而且不能用于提供对特定 DocumentDB 资源的更详细的访问权限。

DocumentDB 资源令牌提供一种安全的方法，允许客户端根据你授予的权限读取、写入和删除你的 DocumentDB 帐户中的资源，而无需主密钥或只读密钥。

以下是典型的设计模式，通过它可以请求、生成资源令牌并将其提供给客户端：

1. 设置中间层服务，以用于移动应用程序共享用户照片。
2. 中间层服务拥有 DocumentDB 帐户的主密钥。
3. 照片应用安装在最终用户移动设备上。
4. 登录时，照片应用使用中间层服务建立用户的标识。这种标识建立机制完全由应用程序决定。
5. 一旦建立标识，中间层服务就会基于标识请求权限。
6. 中间层服务将资源令牌发送回手机应用。
7. 手机应用可以继续使用该资源令牌以该资源令牌定义的权限按照该资源令牌允许的间隔直接访问 DocumentDB 资源。
8. 资源令牌到期后，后续请求将收到 401 未经授权的异常。此时，手机应用会重新建立标识，并请求新的资源令牌。



DocumentDB 资源令牌工作流

## 处理 DocumentDB 用户和权限

DocumentDB 用户资源与 DocumentDB 数据库关联。每个数据库可能包含零个或多个 DocumentDB 用户。下面的代码片段演示如何创建 DocumentDB 用户资源。

//Create a user.  
User docUser = new User  
{  
 Id = "mobileuser"  
};  
  
docUser = await client.CreateUserAsync(UriFactory.CreateDatabaseUri("db"), docUser);

[AZURE.NOTE] 每个 DocumentDB 用户都具有 PermissionsLink 属性，该属性可用于检索与该用户关联的权限的列表。

DocumentDB 权限资源与 DocumentDB 用户关联。每个用户可能包含零个或多个 DocumentDB 权限。权限资源提供对用户在尝试访问某个特定应用程序资源时需要的安全令牌的访问权限。权限资源可能提供两种可用的访问级别：

* 所有：用户对资源具有完全权限
* 只读：用户只能读取资源的内容，但无法对资源执行写入、更新或删除操作。

[AZURE.NOTE] 为了运行 DocumentDB 存储过程，用户必须具有对存储过程将在其中运行的集合的所有权限。

下面的代码片段演示如何创建权限资源、读取权限资源的资源令牌以及将权限与上面创建的用户关联。

// Create a permission.  
Permission docPermission = new Permission  
{  
 PermissionMode = PermissionMode.Read,  
 ResourceLink = documentCollection.SelfLink,  
 Id = "readperm"  
};

docPermission = await client.CreatePermissionAsync(UriFactory.CreateUserUri(“db”, “user”), docPermission); Console.WriteLine(docPermission.Id + " has token of: " + docPermission.Token);

如果你为集合指定了分区键，则除 ResourceLink 以外，集合、文档和附件资源的权限，还必须包括 ResourcePartitionKey。

为了方便地获取与特定用户关联的所有权限资源，DocumentDB 使权限源对每个用户对象均可用。下面的代码片段演示如何检索与上面创建的用户关联的权限、构造权限列表以及代表用户实例化新 DocumentClient。

//Read a permission feed.  
FeedResponse<Permission> permFeed = await client.ReadPermissionFeedAsync(  
 UriFactory.CreateUserUri("db", "myUser"));  
  
List<Permission> permList = new List<Permission>();  
   
foreach (Permission perm in permFeed)  
{  
 permList.Add(perm);  
}  
   
DocumentClient userClient = new DocumentClient(new Uri(endpointUrl), permList);

[AZURE.TIP] 资源令牌的有效时间跨度默认为 1 小时。但是，令牌生存期可以显式指定为最多 5 个小时。

## 后续步骤

* 若要了解有关 DocumentDB 的详细信息，请单击[此处](http://azure.com/docdb)。
* 若要了解有关管理主密钥和只读密钥的信息，请单击[此处](/documentation/articles/documentdb-manage-account)。
* 若要了解如何构造 DocumentDB 授权令牌的信息，请单击[此处](https://msdn.microsoft.com/library/azure/dn783368.aspx)