使用 Azure Key Vault 管理服

务器应用中的机密

- 46 分钟模块7 单元

4.6 (1,617)

对其进行评级

初级开发人员解决方案架构师Azure密钥保管库应用服务

应用程序需要服务密码、连接字符串和其他机密配置值才能完成其工作。 存储和处理机密值是有风险的，并且每次使用都会有泄密的可能性。 Azure Key Vault 与 Azure 资源的托管标识功能相结合，使 Azure Web 应用可以轻松安全地访问机密配置值，而无需在源代码管理或配置中存储任何机密。

学习目标

在本模块中，将执行以下操作：

- 探索 Azure Key Vault 中可存储哪些类型的信息
- 创建 Azure Key Vault 并使用它存储机密配置值
- 从具有 Azure 资源的托管标识的 Azure 应用服务 Web 应用启用对保管库的安全访问
- 实施从保管库中检索机密的 Web 应用程序

简介

- 2 分钟

如果你想了解管理应用配置机密可能出现的问题，那么高级开发人员 Steve 的故事就是最佳选择。

Steve 曾在一家宠物食品配送公司工作了几个星期。 他曾在浏览公司的 Web 应用 — .NET Core Web 应用（该应用使用 Azure SQL 数据库存储订单信息，并使用第三方 API 进行信用卡计费和映射客户地址） — 的详细信息时，不慎将订单数据库的连接字符串粘贴到了公共论坛。

数天后，会计部门发现公司配送了许多无人付款的宠物食品。 有人使用连接字符串访问了数据库，并通过直接更新数据库创建了订单。

在意识到自己的错误后，Steve 急忙更改了数据库密码来阻挡攻击者。 更改密码后，网站开始向用户返回错误：需要更新应用服务器的配置，令其使用新密码。 Steve 直接登录到应用服务器，并更改了应用配置（而不是重新部署），但服务器仍显示失败的请求。 Steve 忘记了该应用的多个实例在不同服务器上运行，而他仅更改了一个服务器的配置。 需要完全重新部署，导致故障时间延长 30 分钟。

但对 Steve 而言幸运的是，会计部门快速纠正了错误，因此只影响了一天的订单。 但他不可能总是这么幸运，因此需要找到一种方法来改进应用的安全性和可维护性。

泄漏数据库连接字符串、API 密钥或服务密码可能导致灾难性后果。 潜在后果包括数据被盗取或删除、财务损害、应用故障时间以及对业务资产和信誉造成无法弥补的损害。 遗憾的是，机密值

通常需要同时在多个位置进行部署，并需要在不适当的时候进行更改。 但总得将这些信息存储在某处！ 让我们看看 Steve 如何通过 Azure Key Vault 降低风险、提升其应用安全性和可维护性吧。

学习目标

在此模块中，你将：

- 了解 Azure Key Vault 中可存储哪些类型的信息。
- 创建 Azure Key Vault 并使用它存储机密配置值。
- 从具有 Azure 资源的托管标识的 Azure 应用服务 Web 应用启用对保管库的安全访问。
- 实现从保管库中检索机密的 Web 应用。

下一单元: 什么是 Azure Key Vault?

继续

什么是 Azure

e Key Vault?

- 5 分钟

Azure Key Vault 是一种机密存储区，一种用于存储应用机密的集中式云服务；应用机密即必须始终安全的配置值，例如密码和连接字符串。 Key Vault 通过将应用机密保存在一个中心位置，并提供安全访问、权限控制和访问日志记录，来帮助控制这些机密。

播放 Azure Key Vault Overview
01:57

使用 Key Vault 的主要好处有以下几点：

- 将敏感应用信息与其他配置与代码分离，从而降低意外泄漏的风险

- 通过为需要访问权限的应用和个人定制的访问策略实现有限制的机密访问
- 集中式机密存储，只允许在一个位置进行所需的更改
- 访问日志记录和监视，帮助你了解在何时以何种方式访问了机密

机密存储在独立的保管库中，保管库是用于将机密组合在一起的 Azure 资源。 机密访问和保管库管理是通过 REST API 完成的，它受到所有 Azure 管理工具和多种常用语言的客户端库支持。 每个保管库具有托管其 API 的唯一 URL。

重要

Key Vault 旨在存储服务器应用的配置机密。 它并非用于存储属于应用用户的数据，也不应该用于应用的客户端部分。 这反映在其性能特征、API 和成本模型中。

用户数据应存储在其他位置，例如使用透明数据加密的 Azure SQL 数据库或使用存储服务加密的存储帐户。 应用用于访问这些数据存储的机密可保存在 Key Vault 中。

什么是 Key Vault 中的机密?

在 Key Vault 中，机密是字符串的名称/值对。 机密名称的长度必须为 1 至 127 个字符，且仅包含字母数字字符和短划线，并且在保管库中必须是唯一的。 机密值可以是大小不超过 25 KB 的任何 UTF-8 字符串。

提示

秘密名称本身不需要特别机密。 如果实现需要调用，可将其存储在应用的配置中。 这同样适用于保管库名称和 URL。

备注

Key Vault 支持字符串之外的两种其他机密类型 — 密钥和证书 — 并提供特定于其用例的有用功能。 此模块不涉及这些功能，而是专注于密码和连接字符串等机密。

保管库身份验证和权限

Azure Key Vault 的 API 使用 Azure Active Directory 来验证用户身份和应用。 保管库访问策略基于操作，且应用于整个保管库。 例如，如果某应用具有保管库的 Get（读取机密值）、List（列出所有机密的名称）和 Set（创建或更新机密值）权限，则该应用可在该保管库中创建机密、列出所有机密名称，并获取和设置所有机密值。

保管库上执行的所有操作都需经过身份验证和授权 — 不可授予任何类型的匿名访问权限。

提示

在向开发人员和应用授予保管库访问权限时，仅授予所需的最低限度的权限。 借助权限限制，可帮助避免代码 bug 所导致的故障，同时减少因凭证被盗或向应用注入恶意代码所带来的影响。

开发人员通常只需要开发环境保管库的“Get”和“List”权限。 某些工程师需要完整权限，以便在必要时更改和添加机密。

对应用而言，通常只需要“Get”权限。 一些应用可能需要“List”权限，具体视应用实现方式而定。 我们在本模块的练习中实现的应用需要“List”权限，这是由应用用于从保管库读取机密的技术决定的。

下一单元: 练习 - 创建 Key Vault 并存储机密

针对 Azure 资源使用托管标识

进行的保管库身份验证

- 4 分钟

Azure Key Vault 使用 Azure Active Directory 对尝试访问保管库的用户和应用进行身份验证。 若要授予 Web 应用访问保管库的权限，首先需要使用 Azure Active Directory 注册应用。 注册将为应用创建标识。 应用拥有标识后，我们便可以向应用分配保管库权限。
Key Vault 使用 Azure Active Directory 身份验证令牌对应用和用户进行身份验证。 从 Azure Active Directory 获取令牌需要机密或证书，因为具有令牌的任何人都可以使用应用标识来访问保管库中的所有机密。
虽然应用机密在保管库中较为安全，但我们仍需在保管库外部保存机密或证书，以便对其进行访问！ 此问题称为“启动问题”，Azure 为此提供了一种解决方案。

Azure 资源的托管标识

Azure 资源的托管标识是一项 Azure 功能，应用可使用此功能访问 Key Vault 和其他 Azure 服务，而无需在保管库之外管理任何机密。 使用托管标识是一种通过 Web 应用利用 Key Vault 的简单、安全方法。
在 Web 应用上启用托管标识时，Azure 会激活专门用于应用的、单独的令牌授予 REST 服务。 应用将通过此服务请求令牌，而不是直接通过 Azure Active Directory 请求令牌。 应用需要使用机密才能访问此服务，但应用服务在启动时会将该机密注入应用的环境变量中。 你无需在任何位置管理或存储此机密值，并且应用外部的任何对象都无法访问此机密或托管标识令牌服务终结点。
Azure 资源的托管标识还会为你在 Azure Active Directory 中注册应用，并在你删除 Web 应用或禁用其托管标识时删除该注册。
托管标识在任何版本的 Azure Active Directory 中均可用，包括 Azure 订阅中包含的免费版。 在应用服务中使用托管标识不会产生额外费用且无需任何配置，并且可以随时在应用中启用或禁用它。
为 Web 应用启用托管标识仅需要单个 Azure CLI 命令，而无需任何配置。 在稍后设置应用服务应用并部署到 Azure 时，将进行此操作。 不过，在此之前，我们将运用托管标识的知识来为应用编写代码。

知识检查

1. 对 Azure 资源使用托管标识会对应用通过 Azure Key Vault 进行身份验证的方式造成什么影响?

该应用使用证书而非机密进行身份验证。

应用的每个用户都必须输入密码。

该应用从令牌服务获取令牌，而不是从 Azure Active Directory 获取令牌。

托管标识由 Azure Key Vault 自动识别，并且会自动进行身份验证。

2. 这些陈述中的哪一项描述了使用 Azure 资源的托管标识向 Key Vault 验证应用的主要优点?

使用托管标识可改善应用程序性能。

使用托管标识，无需在配置过程中处理机密。

托管标识可自动向 Azure Key Vault 授予权限。

检查你的答案