**Azure IoT 中心是什么？**

**连接、监视并控制数百万 IoT 资产**

* 快速入门
* 连接数百万资产
* 支持各种操作系统和协议
* 建立可靠的双向通信
* 提升 IoT 解决方案的安全性

**与数百万 IoT 设备建立双向通信**

依靠 Microsoft Azure IoT 中心轻松安全地连接物联网 (IoT) 资产。使用设备到云的遥测数据，了解设备和资产的状态，在设备需要关注时立即采取措施。在云到设备消息中，可靠地向连接的设备发送命令和通知，并通过确认回执跟踪消息传递。通过持久的方法发送设备消息，以适应间歇性连接的设备。

**使用熟悉的平台和协议**

使用适用于多个平台（包括 Linux、Windows 和实时操作系统）的开放源代码设备 SDK 添加新设备并连接现有设备。使用标准协议和自定义协议，包括 HTTP、高级消息队列协议 (AMQP) 和 MQ 遥测传输 (MQTT)。

**每设备身份验证可提升 IoT 解决方案的安全性**

为每个连接的设备设置标识和凭据，并帮助保持云到设备和设备到云消息的保密性。要保持系统的完整性，请根据需要选择性地撤消特定设备的访问权限。

**通过设备管理，大规模管理 IoT 设备**

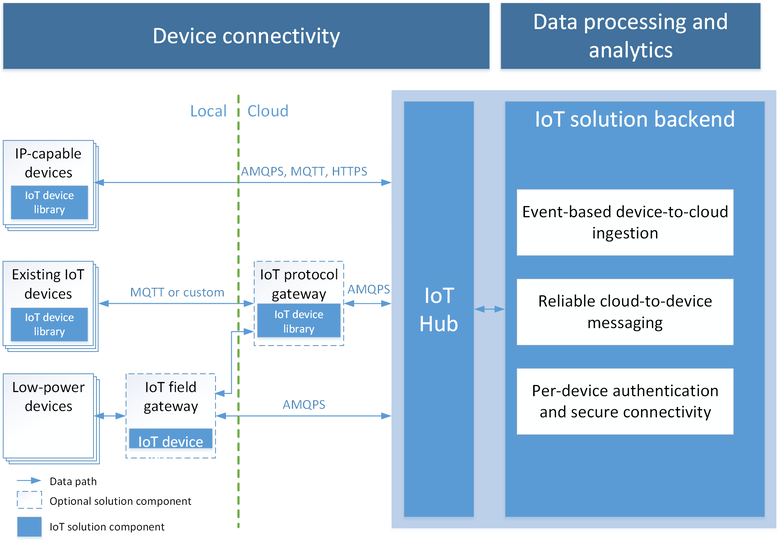
借助 Azure IoT 中心新的设备管理功能，管理员可在云端大规模地远程维护、更新和管理 IoT 设备。免除自定义设备管理解决方案的开发和维护任务，或者无需再花费资源维护全球资产，从而节省了时间和成本。

**通过 Azure IoT 网关 SDK 利用边缘智能**

IoT 网关 SDK 提供强大的框架来生成、配置和部署边缘逻辑，从而让你能够使用 Azure IoT 做更多的事。无论你选择连接旧设备、降低带宽成本、实施安全和因此策略或者任何其他数据处理 — IoT 网关 SDK 都可以简化部署过程，以便让你专心解决真正重要的问题。深入了解[Azure IoT 网关 SDK](https://www.azure.cn/home/features/iot-hub/iot-gateway-sdk/)。

欢迎使用 Azure IoT 中心。本文对 Azure IoT 中心进行了概述，并介绍了应该使用此服务实现物联网 (IoT) 解决方案的原因。Azure IoT 中心是一项完全托管的服务，可在数百万个 IoT 设备和一个解决方案后端之间实现安全可靠的双向通信。Azure IoT 中心：

* 提供多个设备到云和云到设备通信选项，包括单向消息传送、文件传输和请求-答复方法。
* 提供路由到其他 Azure 服务的内置声明性消息。
* 提供设备元数据和同步状态信息的可查询存储。
* 使用每个设备的安全密钥或 X.509 证书来实现安全通信和访问控制。
* 可广泛监视设备连接性和设备标识管理事件。
* 包含最流行语言和平台的设备库。



**NOTE:**

有关 IoT 体系结构的深入讨论，请参阅 [Azure IoT Reference Architecture](http://download.microsoft.com/download/A/4/D/A4DAD253-BC21-41D3-B9D9-87D2AE6F0719/Microsoft_Azure_IoT_Reference_Architecture.pdf)（Azure IoT 参考体系结构）。

**IoT 设备连接性挑战**

IoT 中心和设备库可帮助你应对挑战，即如何以可靠且安全的方式将设备连接到解决方案后端。IoT 设备：

* 通常是无人操作的嵌入式系统。
* 可位于物理访问较昂贵的远程位置。
* 可能只能通过解决方案后端来访问。
* 能力和处理资源可能都有限。
* 网络连接可能不稳定、缓慢或昂贵。
* 可能需要使用专属、自定义或行业特定的应用程序协议。
* 可以使用大量常见的硬件和软件平台来创建。

除了上述需求之外，所有 IoT 解决方案还必须提供可扩展性、安全性和可靠性。使用传统技术（例如 Web 容器和消息传送代理）时，所产生的一系列连接需求不仅难以实现，而且实现起来非常耗时。

**为何使用 Azure IoT 中心**

除丰富的[设备到云](https://www.azure.cn/documentation/articles/iot-hub-devguide-d2c-guidance/)和[云到设备](https://www.azure.cn/documentation/articles/iot-hub-devguide-c2d-guidance/)通信选项（包括消息传送、文件传输和请求-答复方法）外，Azure IoT 中心还通过以下方式解决设备连接问题：

* **设备孪生**。借助[设备孪生](https://www.azure.cn/documentation/articles/iot-hub-devguide-device-twins/)，可以存储、同步和查询设备元数据及状态信息。设备孪生是存储设备状态信息（元数据、配置和条件）的 JSON 文档。IoT 中心为连接到 IoT 中心的每台设备保留一个设备孪生。
* **每个设备的身份验证和安全连接性**。你可以为每个设备设置独有的[安全密钥](https://www.azure.cn/documentation/articles/iot-hub-devguide-security/)，让它连接到 IoT 中心。[IoT 中心标识注册表](https://www.azure.cn/documentation/articles/iot-hub-devguide-identity-registry/)会在解决方案中存储设备标识和密钥。解决方案后端可将个别设备添加到允许或拒绝列表，完全掌控设备访问权限。
* **基于声明性规则，将设备到云消息路由到 Azure 服务**。通过 IoT 中心，可定义基于消息规则的消息路由，控制中心将设备到云消息发送到何处。消息规则不要求编写任何代码，可代替自定义的引入后消息分派程序。
* **设备连接操作监视**。你可以收到有关设备标识管理操作与设备连接事件的详细操作日志。借助此监视功能，IoT 解决方案可识别连接问题，例如，尝试用错误凭据连接的设备、消息发送过于频繁的设备或者拒绝所有云到设备消息的设备。
* **一组丰富的设备库**。[Azure IoT 设备 SDK](https://github.com/Azure/azure-iot-sdks) 适用于各种语言和平台 - C 面向很多 Linux 分发版、Windows 和实时操作系统。Azure IoT 设备 SDK 也支持 C#、Java 和 JavaScript 等托管语言。
* **IoT 协议和可扩展性**。如果解决方案无法使用设备库，则 IoT 中心会公开一个公共协议，它使设备可以通过本机方式使用 MQTT v3.1.1、HTTP 1.1 或 AMQP 1.0 协议。还可以通过以下方式扩展 IoT 中心，以便为自定义协议提供支持：
  + 使用 [Azure IoT 网关 SDK](https://github.com/Azure/azure-iot-gateway-sdk)创建现场网关，该 SDK 可将自定义协议转换为 IoT 中心所理解的三个协议之一。
  + 自定义 [Azure IoT 协议网关](https://github.com/Azure/azure-iot-protocol-gateway/blob/master/README.md)（在云中运行的一个开放源代码组件）。
* **扩展**。Azure IoT 中心可扩展为数百万个同时连接的设备，以及每秒数百万个事件。

**网关**

IoT 解决方案中的网关通常是部署于云中的[协议网关](https://www.azure.cn/documentation/articles/iot-hub-protocol-gateway/)或使用设备在本地部署的[现场网关](https://www.azure.cn/documentation/articles/iot-hub-devguide-endpoints/#field-gateways)。协议网关执行协议转换，例如 MQTT 到 AMQP。现场网关可在边缘运行分析、制定能减少延迟的时间敏感型决策，提供设备管理服务，强制实施安全和隐私约束，还可执行协议转换。这两种网关都可以充当设备与 IoT 中心之间的媒介。

现场网关与简单的流量路由设备（例如网络地址转换设备或防火墙）不同，它通常在解决方案中主动管理访问和信息流。

解决方案可以同时包含协议网关和现场网关。

**IoT 中心如何运作？**

Azure IoT 中心会实现[服务辅助通信](http://blogs.msdn.com/b/clemensv/archive/2014/02/10/service-assisted-communication-for-connected-devices.aspx)模式，以调节设备与解决方案后端之间的交互。服务辅助通信的目标是在控制系统（例如 IoT 中心）与专用设备（部署在不受信任的物理空间中）之间，建立可信任的双向通信路径。该模式会建立下列原则：

* 安全性的优先级高于其他所有功能。
* 设备不接受未经请求的网络信息。设备以仅限出站的方式建立所有连接和路由。若要让设备从解决方案后端接收命令，设备必须定期启动连接，检查是否有任何挂起的命令要处理。
* 设备只能同与它们对等的已知服务（例如 IoT 中心）进行连接或建立路由。
* 设备和服务之间或设备和网关之间的通信路径在应用程序协议层受到保护。
* 系统级别的授权和身份验证以每个设备的标识为基础。它们可让访问凭据和权限近乎实时地撤销。
* 对于因为电源或连接性而导致连接不稳定的设备而言，可通过保留命令和设备通知直到设备连接并接收它们，进而促进其双向通信。IoT 中心会为发送的命令维护设备特定的队列。
* 针对通过网关到特定服务的受保护传输，应用程序有效负载数据会受到单独保护。