MindSphere DevOps 指南 (PRC)

系统手册

03/2019
Version 1.0 (Mar. 2019)

目录

简介 1

1.1 适用范围

本 DevOps 指南仅供 MindAccess Developer Plan 和/或 MindAccess Operator Plan 订户（包括其用户）使用。

这份指南提供了有关应用程序的开发和测试，以及部署和生产运营的信息，并通过相应的 MindAccess 帐户提供应用程序。对于所有应用程序，用户必须满足或超过本 DevOps 指南中指定的所有要求。

所有 MindSphere 应用程序都可以通过阿里云市场销售。有关在阿里云市场中开店以及发布应用程序的流程，请参见阿里云市场 (https://partner.aliyun.com/programs/marketplace) 网站。

本 DevOps 指南中描述的要求和建议仅提供部分信息，并且仅作为 MindSphere 协议中其它部分所述要求的补充。不应将这些要求和建议视为以任何方式限制、约束 MindSphere 协议中其它部分规定的要求或与之相冲突。

本指南“按原样”提供，并将不时更新。本指南中的信息（包括 URL 和其它网站引用）如有更改，恕不另行通知。本指南已经过审核，与所述服务保持一致。

阿里云将努力使这份文件保持准确和最新，但由于 MindSphere 的快速发展，将无法完全排除不一致。我们会定期审核本 DevOps 指南中的信息，并在后续版本中包含必要的更正。

1.2 相关参考资料

在开发应用程序时，必须查看并考虑以下文档中列出的信息：

开发人员文档 (https://developer.mindsphere.io)

MindSphere API 参考 (https://developer.mindsphere.io)

MindSphere 营销指南 (https://siemens.mindsphere.io/terms/)

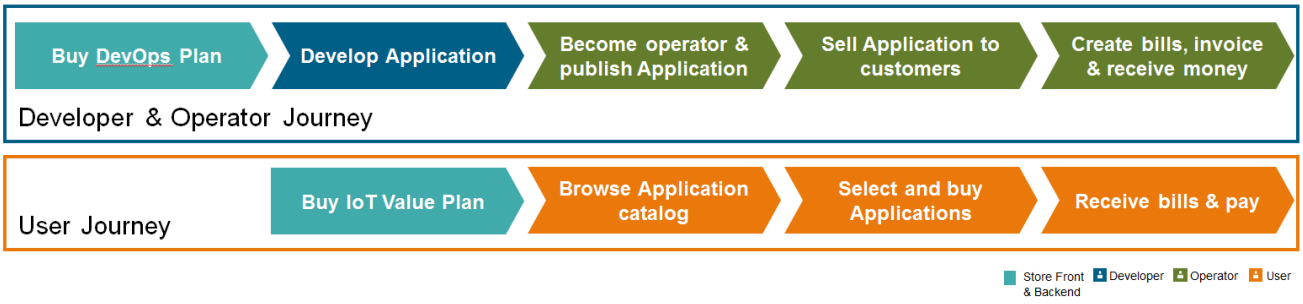
用户文档 (https://documentation.mindsphere.io)

您与阿里云的合同协议。

开发、运营和销售流程

2

端到端流程通常适用于开发应用程序、实施运营并将其提供给其它方，具体的图例说明如下：



为了使您的应用程序商业化，通常必须采取以下步骤。

开发人员角度

1. 订阅 MindAccess DevOpsPlan。
   - 对于 Cloud Foundry 应用程序：

     从阿里云订购并获取 MindAccess Developer Plan。这样便可访问 Cloud Foundry 开发空间。

     借助 MindAccess Operator Plan ，用户可以访问平台上的 Cloud Foundry 生产空间。
   - 对于自托管应用程序：

     从阿里云订购并获取 MindAccess Developer Plan 和出站流量升级服务，以便开发和测试自托管应用程序。

     借助 MindAccess Operator Plan，用户可以访问平台上的生产空间。
2. 配置开发环境。
   - MindSphere 管理型环境

     使用 Cloud Foundry 命令行接口或所选工具来准备开发空间。

     配置 Cloud Foundry 以及单独订购或包含的后端服务，如附加数据存储或消息队列。
   - 自管型环境

     根据需求和规范（可能由环境供应商提供）配置和使用开发环境。
3. 开发应用程序。
   - 根据需求，通过安装适当的软件工具来创建本地开发环境。
   - 有关如何创建应用程序的信息，请参见《开发人员文档》。
   - 有关如何实现 API 调用的信息，请参见 MindSphere API 参考和 API 指南。
   - 使用其中一种受支持的语言创建应用程序。
4. 使用开发空间中的租户来测试和评估应用程序。
   - 按《开发人员文档》中的说明注册应用程序。

     针对预期内容与行为测试和评估应用程序的技术、功能、性能、安全性和用户界面。
   - 使用工具和流程来管理应用程序测试。

运营商角度

1. 订阅 MindAccess DevOpsPlan。
   - 对于 Cloud Foundry 应用程序：

     借助 MindAccess Operator Plan，用户可以访问平台上的 Cloud Foundry 生产空间。
   - 对于自托管应用程序：

     从阿里云订购并获取 MindAccess Operator Plan 和出站流量升级服务。

     借助 MindAccess Operator Plan，用户可以访问平台上的生产空间。
2. 准备访问应用程序。

   出于生产目的，应当使用与应用程序相关的生产系统。因此，应遵循适用于 Cloud Foundry 和自托管应用程序的相应流程。
   - 运营商可以使用 Operator Cockpit 在生产环境中部署和启用应用程序。

     对于自托管应用程序，只需使用 Operator Cockpit 进行注册。
   - 最后，运营商可以使用 Operator Cockpit 从 MindAccess IoT Value Plan 帐户访问应用程序。
3. 操作和使用应用程序
   - 当开发交互式应用程序时，可以在生产租户帐户的 Launchpad 上访问此应用程序。
   - 进行持续监控以保持应用程序的健康状态。
   - 保持应用程序为最新状态（例如，开源软件、Cloud Foundry 中用于 Java 和 Node.js 的最新构建包、后端服务更新）。

卖方角度

1. 订阅 MindAccess DevOpsPlan。
2. 部署应用程序。
3. 注册应用程序。
4. 在阿里云市场 (https://partner.aliyun.com/programs/marketplace)注册为卖方并开店。
5. 在商店中输入应用程序的产品信息。
6. 向 MindSphere 营销团队提出申请以将您的应用程序在 MindSphere 商店中列出。

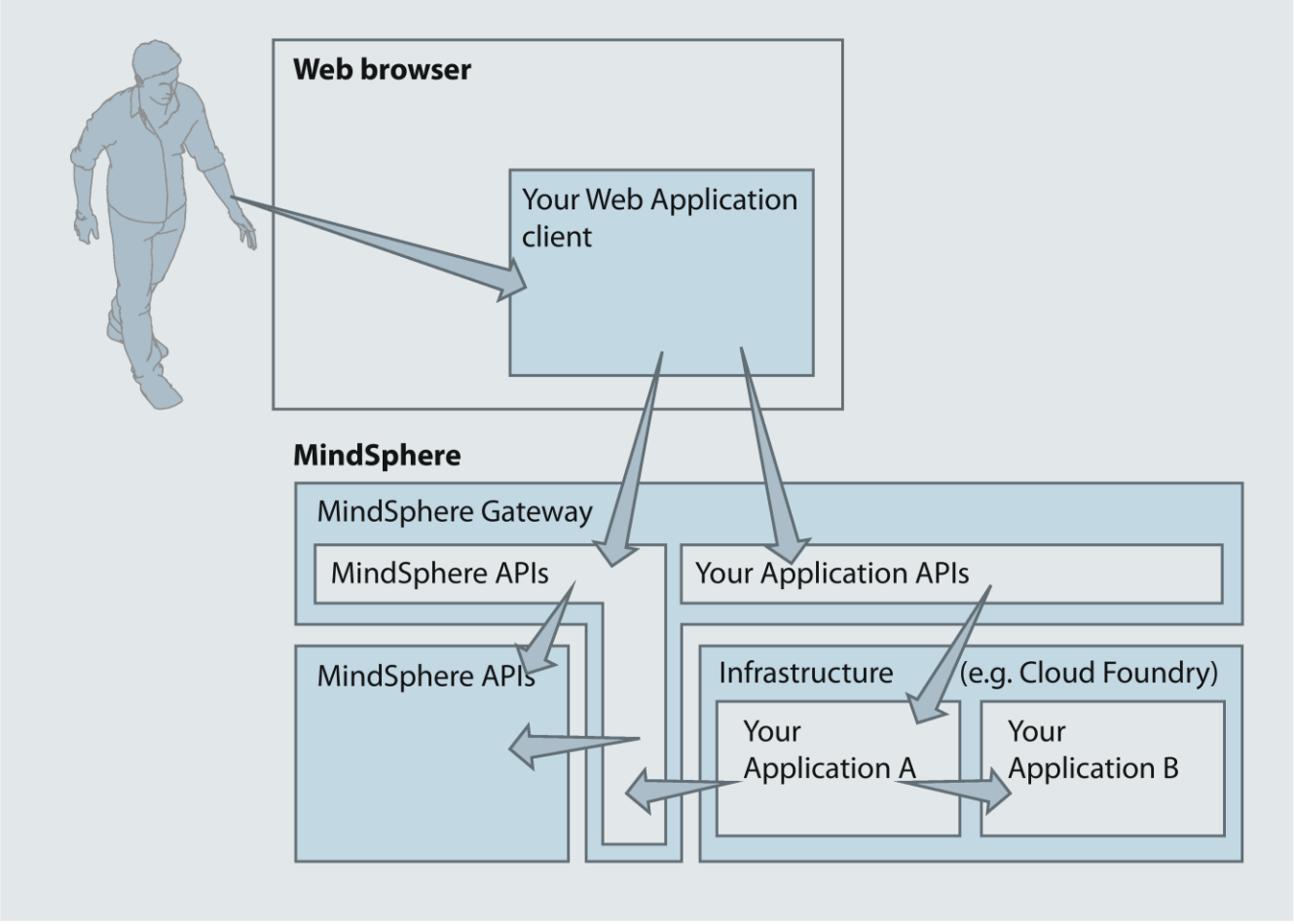
MindSphere 平台服务

3

3.1 简介

MindSphere 提供各种支持服务来加速应用程序开发。可通过名为 MindSphere Gateway 的网关服务访问基于 MindSphere API 的服务，此网关用于管理客户的调用路径和应用程序可用性。下图示例说明了 Web 应用程序的调用路径。

以下部分描述了我们通过 MindSphere API 公开的服务访问、应用程序注册、调用路径和一般开发指南。



3.2 使用 MindSphere API

MindSphere API 公开 RESTful 服务，例如“时间序列”或“资产管理”。我们服务的订户可以根据订阅使用 MindSphere API。

使用 MindSphere API 时，必须遵守以下要求：

- 平台提供的 API 只能以 API 参考中所述的方式加以使用，并且只能用于其中所述的目的。
- 只能根据 API 参考中所述的方式使用 API 调用。
- 请注意，由于未来的功能增强和平台发展，将对 MindSphere API 进行相应更改。我们将尽一切努力避免更改，并在预计进行更改时提前通知您。

参见

相关参考资料 (页 3)

3.3 应用程序调用路径和 MindSphere Gateway

应用程序的调用路径

对 MindSphere API 的任何访问都必须使用 MindSphere Gateway。根据您开发的是具有浏览器客户端的 Web 应用程序还是纯后端应用程序，对 API 的访问将有所不同，《开发人员文档》中介绍了相关信息。

Web 应用程序浏览器客户端可以

- 调用 MindSphere API。这些调用必须指向以下架构的 URL：

  ```
  <web-app-host>/api/<api-name>[-<api-provider>]/v<major>/<endpoint>
  ```

- 调用您自己的应用程序 API。这些调用必须指向以下架构的 URL：

  ```
  https://<tenant>-<webapp>[-<provider>].<region>.mindsphere-in.cn/[<path>]
  ```

MindSphere 后端应用程序可以

- 使用从授权服务器获取的服务凭证访问令牌调用 MindSphere API。这些调用必须指向以下架构的 URL：

  ```
  https://gateway.<region>.mindsphere-in.cn/api/<api-name>[-<api-provider>]/v<major>/<endpoint>
  ```

- 使用从浏览器客户端调用获取的访问令牌调用您自己的其它后端应用程序。

MindSphere Gateway 的可用性

为了使应用程序在 MindSphere Gateway 中可用，必须使用以下命名约定。

从 Web 应用程序客户端调用时需遵循以下架构：

```
https://<tenant>-<webapp>[-<provider>].<region>.mindsphere-in.cn/[<path>]
```

将路由到采用如下形式的内部 URL

```
https://<application>-<tenant-id>.apps.cn1.mindsphere-in.cn
```

Cloud Foundry

为了使应用程序可以从 Web 应用程序客户端调用，需要创建一个基于 Cloud Foundry 的应用程序，将其命名为 `<application>-<tenant-name>`，其中 `<tenant-name>` 为租户名称（即，MindAccess Developer 帐户或 MindAccess Operator 帐户的 URL，具体视情况而定），`<application>` 为 Web 应用程序客户端调用中要用作路径参数的名称。

开发和运营通用指南

4

在不影响所有其它要求的情况下，您的应用程序必须始终遵循以下规定：

- 不得用作软件的分发机制，或者包含在此类应用程序中创建或启用软件商店、分销渠道或其它软件交付机制的特性或功能。这些限制不包括允许向浏览器传递客户端代码的 Web 应用程序。
- 不得使用过时的软件组件和构建包，包括但不限于开源软件。
- 必须使用最新的软件组件（例如，Cloud Foundry 中用于 Java 和 Node.js 的最新构建包、后端服务更新）。只要有可用更新，就必须立即应用这些更新。禁止使用具有已知漏洞的任何软件组件。
- 在服务不可用或者服务发生硬件或系统故障时，必须确保任何内容，特别是应用程序能够自动重启而无需运营商手动干预。此外，还必须以能够在系统重新启动时恢复运行状态的方式构建应用程序。
- 如果发现任何软件漏洞，为确保其它用户的安全，我们可能会阻止访问您的应用程序。
- 您全权负责应用程序的维护。
- 必须在分配到 MindAccess Developer 帐户或 MindAccess Operator 帐户的 URL 子域下部署应用程序，具体视情况而定。
- 部署 Cloud Foundry 应用程序时，必须为每个应用程序创建一个空间。

数据处理

处理数据（包括个人数据）时，您有责任遵守适用法律和 MindSphere 协议的条款，并满足客户预期。请公开关于访问的数据类型以及应用程序如何处理和保护这些数据类型的信息，并确保您的客户已同意此类访问和处理。

设计考虑事项

在开发应用程序时，应考虑以下建议。

12-Factor 应用程序

强烈建议遵循 12-Factor 方法。

失败、错误和异常

始终处理错误和异常。确保应用程序在出现异常和错误时能正常退出。记录错误和异常时，建议使用关联 ID。

容错

服务调用和资源访问应考虑到所请求的服务可能并非始终可用。因此，有必要实现适当的重试机制。

可扩展性

必须根据具体的并发和负载要求，通过运行多个实例来实现应用程序和服务的水平扩展。云基础架构服务应用程序应当用于水平扩展。

应用程序健康

您的应用程序应该实现某种“健康”接口或机制，以验证应用程序不仅在运行而且功能完整。对所有应用程序使用相同的约定，这样可以建立全局健康跟踪和监视。

安全义务

5

5.1 简介

在不影响所有其它要求的情况下，您需要遵循安全最佳实践要求并实现和维护安全机制，以便达到预期的应用程序安全级别，以及支持平台、连通网络和设备的完整性。这包括必须遵循本章中规定的安全义务。

5.2 访问控制

- 您将获得一个适用于应用程序的访问令牌，以便使用基于 MindSphere API 的服务。此访问令牌仅可用于预期目的。禁止将此访问令牌用于所有其它用途。
- 在 MindSphere 平台上运行的应用程序随 JSON Web Tokens（缩写为“JWT”）一起提供。必须根据 rfc7519 验证 JWT。必须拒绝 JWT 无效或缺失的所有请求。
- 必须采取一切必要措施来保护访问令牌，以避免未经授权的第三方使用该令牌。如果发现有未经授权方可以访问此类访问令牌的风险，必须立即给 security@mindsphere.io 发送电子邮件。
- 必须定期更改密码。
- 必须定期更改所使用的密码，以便使用我们的服务。如果没有另行规定和书面形式许可，密码更改间隔不得超过 12 个月。

5.3 所提供服务的安全性

在任何情况下，都不得利用服务来：

- 对所提供服务的受限部分进行未经授权的访问。
- 拦截（被动或主动）所提供服务受限部分的数据流。
- 篡改或伪造所提供服务的安全机制。这包括伪造协议标头（例如，IP、TCP 或 UDP）以及非法使用所提供服务来隐藏某些活动（例如，通过所提供服务使用代理或者提供冒名或匿名网络节点）。
- 使用所提供服务来发布、发送或方便发送未经请求的群发电子邮件或其它消息、促销、广告或恳请（“垃圾邮件”），包括商业广告和信息公告。
- 访问或减少所提供服务的其它用户的资源（计算、存储等）。

5.4 确保提供安全服务

任何违反本 DevOps 指南中列出的要求或滥用所提供服务的行为都可能受到我们的调查。可能采取以下措施：

- 删除、禁止访问或修改违反本 DevOps 指南或任何其它有关所提供服务的协议的任何内容或资源。
- 向有关当局举报任何已知或怀疑违反法律或法规的活动。
- 与执法机关合作，包括向执法当局举报相关的安全违规行为。

5.5 举报违规行为

如果发现或遇到任何违反本 DevOps 指南的行为，必须立即通知并按要求提供帮助以停止或纠正违规行为。

要举报任何违反本 DevOps 指南的行为，请通过将电子邮件发送到 security@mindsphere.io 来联系我们。

风格指南

6

为了保持一致的外观，您的应用程序必须符合 Operator Cockpit 中规定的要求。有关风格指南和规范的更多详细信息，请参见 Operator Cockpit 文档。Operator Cockpit 针对以下方面设定了规范和要求：

应用程序图标和显示名称

应用程序图标

您的应用程序图标是传达应用程序优势的首要途径。在 MindSphere 中，您需要进行输入以便为应用程序创建唯一图标。您的注册公司名称必须附加到应用程序图标上，以清楚地表明您是该应用程序的提供方。应用程序图标的设计必须与阿里云作为服务（例如 Asset Manager、Fleet Manager）一部分使用的图标设计明显不同。

显示名称

每个应用程序必须具有唯一的显示名称。应用程序的名称非常重要，因为潜在客户可通过此名称清楚地了解该应用程序提供的服务。

应用程序用户界面

当通过 MindSphere URL 向 MindAccess IoT Value Plan 的订户提供应用程序时，应用程序 Web 前端必须提供以下元素：

- 必须通过剪切到应用程序中的代码来集成 MindSphere OS Bar。MindSphere OS Bar 为用户提供重要的核心功能，如“主页按钮”。有关如何集成 MindSphere OS Bar 的信息，请参见《开发人员文档》。
- 包含公司名称、电话号码或电子邮件地址的控件，该控件描述如何获取应用程序的服务和支持。对于您的应用程序，该控件不允许引用阿里云或西门子。

当通过非 MindSphere URL 向第三方提供自托管应用程序时，应用程序 Web 前端不得

- 集成 MindSphere OS Bar 或其任何部分。
- 以任何方式引用阿里云或西门子。这包括但不限于设计和内容。

品牌化

- 不得使用与西门子相关的名称，例如“西门子”、“Si”以及与“西门子”名称类似的任何引用，包括但不限于 SIMATIC、SINUMERIK、SINALYTICS 及其任何缩写，与西门子相关的徽标或易混淆的任何单词或徽标，但本协议中另有明确规定的除外。
- 除非此处另有明确规定，否则不得将您的解决方案名称或者任何商标或商品名称与任何西门子产品直接或间接组合使用或并列使用，也不得在其中进行引用。
- 您只能在经过我们事先单独书面同意的情况下使用西门子的商标或商品名称，如本指南中所述，或者按您的具体要求另行提供。西门子的商标和商品名称包括但不限于 MindSphere、MindConnect、MindApps、MindAccess、MindServices 以及以“Mind”开头的其它名称。
- 不得使用与阿里云相关的名称，例如“阿里巴巴”、“阿里云、 “阿里” ”以及与“阿里云”名称类似的任何引用，及其任何缩写，与阿里云相关的徽标或易混淆的任何单词或徽标，但本协议中另有明确规定的除外。
- 除非此处另有明确规定，否则不得将您的解决方案名称或者任何商标或商品名称与任何阿里云产品直接或间接组合使用或并列使用，也不得在其中进行引用。
- 您只能在经过我们事先单独书面同意的情况下使用阿里云的商标或商品名称，如本指南中所述，或者按您的具体要求另行提供。

参见

相关参考资料 (页 3)