智能开发助手

产品介绍

文档版本 01

发布日期 2024-10-15

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 什么是智能开发助手

CodeArts Snap是基于盘古研发大模型的智能开发助手，重塑了智能化软件研发的新范式，让开发者更加聚焦业务创新，事半功倍。CodeArts Snap是基于智能生成、智能问答2大核心能力，覆盖了代码生成、研发知识问答、单元测试用例生成、代码解释、代码注释、代码调试、代码翻译、代码检查等开发场景，释放软件研发生产力。

2 产品优势

1. 高效提升编码效率和质量。CodeArts Snap能够将自然语言转化为规范可阅读、无开源漏洞的安全编程语言，从而提升开发者的编码效率和质量。

   图 2-1 代码生成示例

```
/**
 * 打开弹窗，可以点击确认和关闭
 */
onOperableNodeEdited(node) {      You, 现在 • Uncommitted changes
  const results = this.dialogService.open({
    id: 'dialog-service',
    width: '30px',
    maxHeight: '60px',
    title: '确认操作',
    content: '确认选择的操作？',
    backdropCloseable: false,
    dialogtype: 'standard',
    buttons: [
      {
      cssClass: 'primary',
      text: '确定',
      handler: ($event: Event) => {
        this.onOperableNodeConfirmed(node);
      }
    ],
    {
      text: '取消',
      cssClass: 'common',
      handler: ($event: Event) => {
        results.modalInstance.hide();
      }
    },
    data: node
  });
}
```

2. 功能强大且全面。CodeArts Snap覆盖了代码生成、研发知识问答、单元测试用例生成、代码解释、代码注释、代码翻译、代码调试、代码检查八大功能，能够满足开发者开发过程中的不同需求和开发场景。

图 2-2 代码解释

【代码解释】：

```
/**
   * 获取用户云龙项目，是否是新用户，有config权限的云龙项目，操作资源等数据
   * @returns
   */
  getGroups(): Observable<any> {
    let res = {
      content: {
        group: [],
        configPrivilegeGroups: [],
        operations: '',
        ifAdmin: false,
        isNewUser: false,
        isProjectExist: true
      },
      exceptionData: null,
      status: 'ok'
    };

    return new Observable(observable => {
      let queryConfigProject = this.getUserConfigProject();
      let queryUserOperation = this.getUserOperationBySpaceUuid(this.projectDetailInfoService.getProjectSpaceUUID());
      let queryAdminOrNew = this.getUserAdminOrNew();
      let queryProjectExist = this.getSpaceIsExist(this.projectDetailInfoService.getProjectSpaceUUID());
      forkJoin([queryConfigProject, queryUserOperation, queryAdminOrNew]).subscribe(
        ([configProjectRes, operationRes, adminOrNewRes]) => {
          queryProjectExist.subscribe(projectExistRes => {
            if (this.checkResStatus([configProjectRes, operationRes, adminOrNewRes, projectExistRes])) {
              res.content = this.makeUpUserAuthorData(configProjectRes, operationRes, adminOrNewRes, projectExistRes);
            }
            observable.next(res);
            observable.complete();
          });
        },
        error => {
          observable.error(res);
          observable.complete();
        }
      );
    });
  }
```

代码的功能和目的:获取用户的云项目信息,判断是否为新用户,获取具有配置权限的云项目,操作资源等数据。
代码的主要逻辑如下:
1.创建一个名为getGroups的方法,返回一个Observable<any>对象。
2.在方法内部,创建一个名为res的对象,该对象包含content、exceptionData和status三个属性。
3.content属性是一个对象,包含group、configPrivilegeGroups、operations、ifAdmin、isNewUser、isProjectExist七个属性。
4.exceptionData属性是一个null类型的值。
5.status属性的值为'ok'。
6.使用Observable创建一个观察者对象,并返回该对象。
7.在观察者对象中,执行以下操作:
1.调用getUserConfigProject方法获取配置云项目的信息,并将结果赋值给queryConfigProject变量。
2.调用getUserOperationBySpaceUuid方法获取用户操作云项目的信息,并将结果赋值给queryUserOperation变量。
3.调用getUserAdminOrNew方法获取用户是否为管理员或新用户的信息,并将结果赋值给queryAdminOrNew变量。
4.调用getSpaceIsExist方法判断云项目是否存在,并将结果赋值给queryProjectExist变量。
5.使用forkJoin方法并发地订阅queryConfigProject、queryUserOperation和queryAdminOrNew这三个观察者对象。
6.在每个观察者对象的回调函数中,通过subscribe方法分别订阅configProjectRes、operationRes和adminOrNewRes这三个结果。
7.在configProjectRes的回调函数中,通过subscribe方法订阅projectExistRes的结果。
8.在projectExistRes的回调函数中,判断checkResStatus方法的返回值。
9.如果返回值为true,则调用makeUpUserAuthorData方法生成用户的认证数据,并将其赋值给res.content属性。
10.通过observable.next方法将res对象推送给观察者对象。
11.通过observable.complete方法结束观察者对象的生命周期。
12.如果出现错误,通过observable.error方法将res对象推送给观察者对象。
13.通过observable.complete方法结束观察者对象的生命周期。
以上是该段代码的主要逻辑。

3. 智能生成和问答。CodeArts Snap具备智能生成和智能问答的核心功能，可以根据中英文描述生成完整的函数级代码，同时提供代码的自动检查和修复。

图 2-3 研发问答示例

3 功能特性

- 支持多种编程语言，并能根据开发者键入的函数签名和注释自动生成函数体。
- 支持根据行级注释或代码上下文信息自动生成与描述场景匹配的代码。
- 可根据开发者当前光标位置的前后语句片段进行代码填空和补全。
- 支持跨文件生成与任务相关的代码。
- 支持从功能、目的和实现逻辑三个维度对代码进行解释说明。
- 可根据用户需求内容生成行级、函数级注释信息，能够帮助开发人员高效补充代码注释。
- 可根据输入的代码和错误信息，得到错误原因并给出修复方案。
- 支持生成高覆盖率的单元测试代码，包括单个方法和类级别的单元测试框架代码。
- 可根据提问来检索研发相关知识，提供答案。
- 支持对代码进行函数级检查功能，可及时、主动发现编码缺陷，提升代码质量和安全性。
- 支持代码翻译，可以指出不同语言关键元素差异，帮助开发者适应新环境。

4 安全

4.1 责任共担

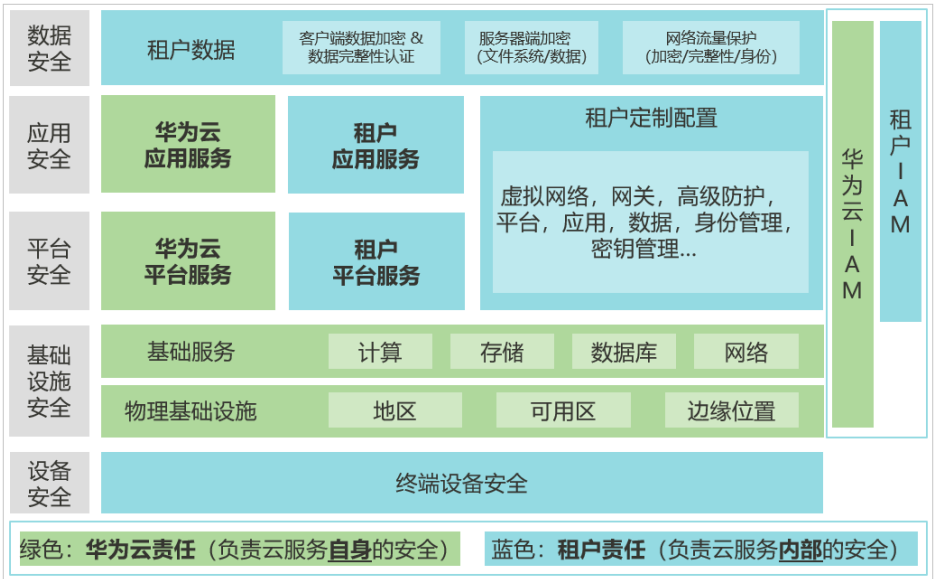
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如**图4-1**所示。

- 华为云：负责云服务自身的安全，提供安全的云。华为云的安全责任在于保障其所提供的IaaS、PaaS和SaaS类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- 租户：负责云服务内部的安全，安全地使用云。华为云租户的安全责任在于对使用的IaaS、PaaS和SaaS类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《华为云安全白皮书》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 4-1 华为云安全责任共担模型



4.2 身份认证与访问控制

身份认证

Snap公有云使用统一身份认证服务IAM进行认证鉴权，用户需要首先在华为云上注册账号。

CodeArts Snap支持两种认证方式：

- Token认证：通过Token认证调用请求。
- AK/SK认证：通过AK（Access Key ID）/SK（Secret Access Key）加密调用请求。推荐使用AK/SK认证，其安全性比Token认证要高。

访问控制

1. 邀测试用
   - 用户可打开**CodeArts Snap申请邀测页面**，申请邀测权限。
   - 邀测权限审批通过之后，账号管理员（te_admin）可以在**CodeArts Snap成员管理**页面导入用户列表，最多可以导入20个用户。
   - 一个账号下的所有用户默认可以调用CodeArts Snap推理接口2000次/天。
   - 邀测试用时长为30天，超过时长用户的访问权限将会被锁定。

4.3 模型安全

模型开发安全性与合规性

1. 用于模型训练的数据安全性与合规性。
   - 所有用于训练的数据均为开源合规的数据。
   - 所有用于训练的数据均过滤密码、IP地址、手机号、email等个人隐私信息。

- 对所有用于训练的数据集进行版本管理，支持数据溯源；数据集存储安全，且对数据访问进行身份及权限控制，数据访问基于https加密传输，数据访问可防篡改、防泄漏。

2. 模型安全性及合规性。
   - 对模型文件进行版本管理，支持模型溯源；模型训练工作流的访问操作通过身份及权限控制且模型训练、推理所依赖的环境支持租户资源隔离，模型文件存储安全，且对模型文件访问进行身份及权限控制，模型文件访问基于https加密传输，模型训练及访问可防篡改、防泄漏。
   - Snap研发知识问答模型部署前，对模型进行内容合规自评，覆盖涉政、违法、诈骗、宗教、低俗暴力、社会负面、敏感信息等问题及角色扮演、反面诱导等12种对抗攻击方式的测评，识别模型生成内容的合规风险，持续强化模型合规训练。

模型运行安全性

1. 通过流控策略进行单用户限流和总并发限流，同时对推理请求的上下文窗口大小进行限制，防止模型资源被滥用。
2. 模型推理API访问基于https加密传输，且访问经过身份认证及鉴权。
3. 模型运行所依赖的环境支持租户资源隔离。

模型应用安全性、数据隐私保护及合规性

1. 具备外部攻击防护能力，基于https加密传输保证模型输入输出数据安全；通过网关流控进行DDos防护；通过身份认证及鉴权进行访问控制，防止未授权的访问。
2. 具备租户数据保护机制，不使用租户数据用于模型训练；不存储租户敏感隐私数据，如身份信息、密码等；不同租户间数据隔离，不可共享；支持根据租户授权情况存留租户数据，存留期结束，立即删除租户数据。
3. 具备内容合规风控机制，支持对用户输入、模型输出内容进行内容合规风险检测，自动识别政治敏感、社会歧视等18类合规风险，提供健康的模型服务；同时CodeArts Snap生成的内容只是建议内容，需要用户对内容进行审核。

模型安全运维与运营

1. 外部请求和系统操作记录安全审计日志；日志打印合规，对敏感信息脱敏打印。
2. 具备账号封禁机制，可对存在恶意行为账号进行服务使用限制。
3. 具备用户监督机制，提供用户反馈通道，支持对使用过程中发现的问题进行反馈；服务侧根据用户的反馈，进行对应的安全运营。

5 约束与限制

本节介绍了CodeArts Snap中的限制，如表5-1所示

表 5-1 使用限制说明

指标类型	指标项	限制说明
IDE版本	版本要求	目前适配的主流IDE类型及版本要求包括： • IntelliJ IDEA版本要求2021.3及以上。 • PyCharm版本要求2021.3及以上。 • VS Code版本要求1.69.0以上。 • CodeArts IDE版本要求2.3.0 及以上。
add to chat的代码长度	代码长度（字符）	代码长度<=10000。
对话框的输入文本长度	文本长度（字符）	<=2000。
模型的token数限制	数量限制（token）	<=4096，当输入及输出总的token数达到上限后，模型无法返回新的内容，可能导致返回代码或文本不完整。
单用户访问速度限制	速度限制（请求数/每分钟）	单用户访问速度限制60次/每分钟。