代码托管

产品介绍

文档版本 01

发布日期 2023-09-05

华为技术有限公司

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。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

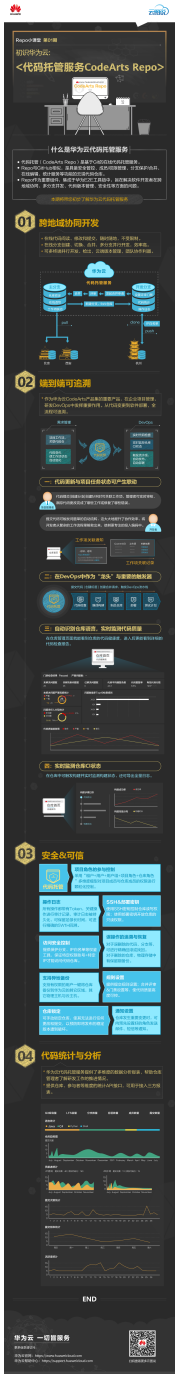
客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

1 图解 CodeArts Repo 1
2 什么是代码托管 3
3 产品优势 5
4 应用场景 7
5 功能特性 8
5.1 极致安全韧性 8
5.2 支持 Git 多种作业流 9
5.3 多形式代码检视 9
5.4 代码上库质量门禁 10
5.5 围绕代码研发资产追溯 10
5.6 内嵌仓库规范和模板 11
6 安全 12
6.1 责任共担 12
6.2 身份认证与访问控制 13
6.3 数据保护技术 14
6.4 审计与日志 16
6.5 监控安全风险 17
6.6 安全运维 17
6.7 认证证书 18
7 约束与限制 19

1 图解 CodeArts Repo



2 什么是代码托管

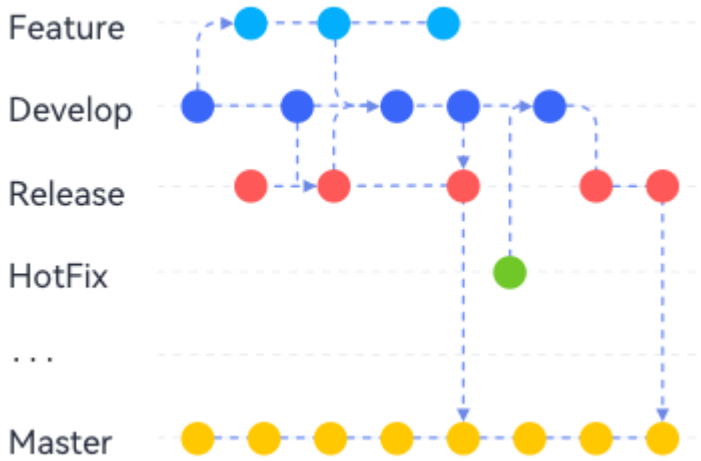
服务概述

代码托管（CodeArts Repo）是面向软件开发者的基于**Git**的在线代码托管服务，是具备安全管控、成员/权限管理、分支保护/合并、在线编辑、统计服务等功能的云端代码仓库，旨在解决软件开发者在跨地域协同、多分支并发、代码版本管理、安全性等方面的问题。

- 在线代码阅读、修改、提交，随时随地开发，不受地域限制。
- 在线分支管理，包含分支新建、切换、合并，实现多分支并行开发，效率高。
- 分支保护，可防止分支被其他人提交或误删。
- IP白名单地域控制和支持HTTPS传输，拦截不合法的代码下载，确保数据传输安全性。
- 支持重置密码，解决用户忘记密码的问题。

代码托管的工作模式

- 代码托管（CodeArts Repo）采用Git Flow作为基础工作模式。
- Git-Flow提供了一组建议，通过严格执行这些建议的规则，帮助中小型研发团队，能够更好的规范自己的开发工作。
  - **并行开发：**各个特性与修复bug，可以并行。
  - **团队协作：**多人开发过程中，大家都能够理解其他人的当前工作。
  - **灵活调整：**通过Hotfix分支，支持各种紧急修复的情况。



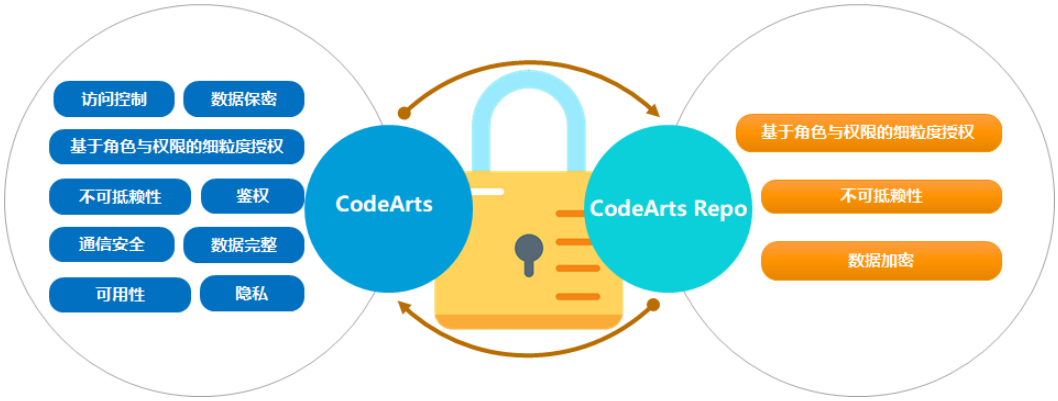
- **master分支：**最为稳定，功能比较完整，随时可发布的代码。
- **develop分支：**用于平时开发的主分支，并一直存在，永远是功能最新最全的分支，包含所有要发布到下一个release的代码，主要用于合并其他分支。
- **feature分支：**用于开发新的功能的分支，一旦开发完成，通过测试，合并回develop分支进入下一个release。
- **release分支：**用于发布准备的专门分支。
- **hotfix分支：**用于修复线上代码的bug 。

  说明

  - 所有开发分支从develop分支拉取。
  - 所有hotfix分支从master分支拉取。
  - 所有在master分支上的提交都必须要有tag ，方便回滚。
  - 只要有合并到master分支的操作，都需要和develop分支合并下，保证同步。
  - master分支和develop分支是主要分支，主要分支每种类型只能有一个，派生分支每个类型可以同时存在多个。

3 产品优势

CodeArts 与 CodeArts Repo 的安全优势



CodeArts层面的安全特性：

- **访问控制**：公有云采用“租户+用户+用户组+角色”统一模型对权限进行控制。
- **鉴权**：CodeArts基于公有云统一的认证服务IAM来进行认证。用户通过HTTPS/SSH访问代码仓库，将使用SSH Key或者仓库用户名及密码进行访问鉴权。
- **基于角色与权限的细粒度授权**：不同的角色，在不同的服务中，根据不同的资源，可以有不同的操作权限。还可以做自定义的权限设置。
- **不可抵赖性**：CodeArts基于公有云IAM Token机制，所有操作都必须带有Token，对所有关键操作进行审计记录。审计日志被持久化，可保留足够长时间，并可进行精确的回溯。
- **数据保密性**：对于敏感信息，CodeArts会进行加密等进行存储。
- **通讯安全**：CodeArts对外提供的服务均使用HTTPS、SSH等安全协议，保证了通讯的安全性。
- **数据完整性**：CodeArts的关键信息都保存在内部数据库中，通过事务等各种机制保障了数据的一致性。
- **可用性**：CodeArts的各个服务都是集群方式，通过保证了服务的高可用性。
- **隐私**：CodeArts不涉及到租户及用户的隐私。

代码托管（CodeArts Repo）层面的安全特性：

- **基于角色与权限的细粒度授权**：在CodeArts Repo层面，提供针对代码访问的，更加细粒度的授权模型。
- **不可抵赖性**：我们提供代码仓库的完整访问日志，供用户审计。
- **数据加密**：用户的代码在CodeArts Repo中，是以加密方式存储的。

跨地域协同开发

- 在线代码阅读、修改和提交，随时随地，不受限制。
- 在线分支创建、切换、合并，多分支并行开发，效率高。
- 支持 Git-LFS ，大文件存储无忧；
- 支持在线 Code Review ，团队协作利器。

基于代码的统计分析

- 代码仓库提交信息统计。
- 代码仓库贡献者统计。
- 代码语言统计。

4 应用场景

异地协同开发

- 应用：面向中小企业、孵化中心，协同合作。
- 场景特点：用户群体对开发工作的推进效率，敏捷度要求更高，需要高效的协作管理方式和更低开发成本。面临异地开发协同效率低、代码合并冲突频繁的难题。
- 适用场景：云端代码托管服务，实现协同开发。多分支管理功能和合并请求功能，彻底解决代码合并冲突的难题。

高校教学

- 应用：高校教师与学生，学习与授课。
- 场景特点：目前缺少功能完备的研发工具链，搭建研发工具环境耗费大量时间，环境维护耗费精力，现有的研发工具上手慢，学习成本高，不利于教学。
- 适用场景：代码托管服务提供完整的代码托管服务，以及丰富的代码仓库模板，使学生可以迅速上手。

5 功能特性

5.1 极致安全韧性
5.2 支持Git多种作业流
5.3 多形式代码检视
5.4 代码上库质量门禁
5.5 围绕代码研发资产追溯
5.6 内嵌仓库规范和模板

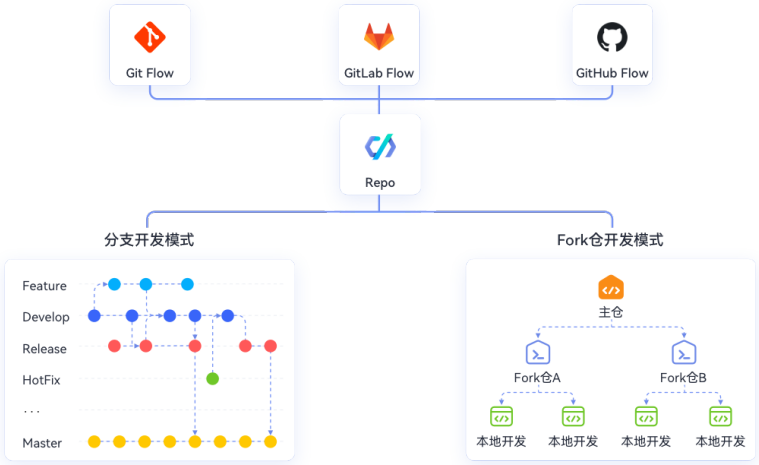
5.1 极致安全韧性

基于云原生架构全栈自研，提供极致韧性和安全的代码托管能力，源于华为多年实践成果，覆盖云、管、端、车、IT等超大产品协同开发，10亿级代码管理，万人团队并发在线协同作业、高并发代码下载，超大存储容量。

5.2 支持 Git 多种作业流

多种开发作业协同方式

提供基于Git的多种开发协作模式，既适合中小企业灵活开发模式，也支持中大型企业的复杂开发协作模式。



5.3 多形式代码检视

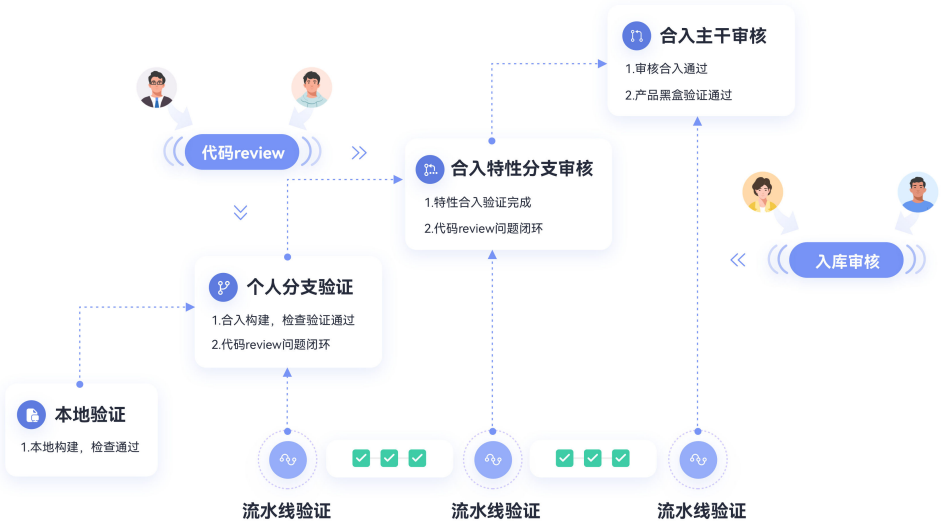
多形式的代码检视活动

支持基于文件的随心检视、合并请求代码检视能力，让团队集中检视或者分散式协同检视，支持检视模板、检视人自动分配、检视任务通知设置，检视意见可跟踪，可闭环，详见**合并请求**。

5.4 代码上库质量门禁

多层级、细粒度代码上库质量门禁

支持人工审核、自动化流水线集成对上库代码进行质量管控，不符合质量指标的代码不允许入库，人工审核支持权责分离原则（SOD），自动化检查，支持分支级管控，详见**合并请求**。



5.5 围绕代码研发资产追溯

围绕代码的研发资产追溯

提供从需求、任务、设计、缺陷、代码、版本的记录追溯，掌握每一行代码的来龙去脉，方便网上问题定位和审计，详见**E2E设置**。

5.6 内嵌仓库规范和模板

丰富的仓库模板，标准化的团队开发活动

提供仓库模板确保团队开发行为统一，更加方便的基于研发数据做效能分析和改进。

6 安全

6.1 责任共担
6.2 身份认证与访问控制
6.3 数据保护技术
6.4 审计与日志
6.5 监控安全风险
6.6 安全运维
6.7 认证证书

6.1 责任共担

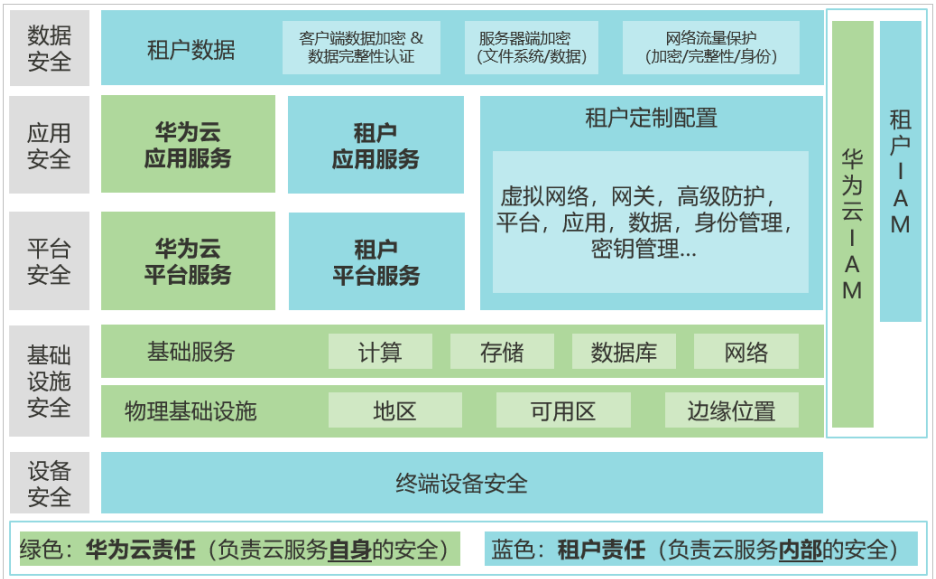
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如**图6-1**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，以及身份帐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 6-1 华为云安全责任共担模型



6.2 身份认证与访问控制

身份认证

无论通过管理控制台或API接口访问CodeArts Repo，CodeArts Repo使用统一身份认证服务IAM进行认证鉴权。

CodeArts Repo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。

关于认证鉴权的详细介绍及获取方式，请参见**认证鉴权**。

访问控制

1. **IAM权限管理**

   权限管理是基于角色与权限的细粒度授权，即根据不同角色的工作需要分配不同的操作权限，用户只可访问被授权资源。

   CodeArts Repo中的角色有仓库管理员/创建者，Committer，开发者，浏览者。

   - 仓库管理员/创建者/Committer支持对仓库成员进行管理，更新仓库代码并对仓库配置进行设置等操作；
   - 开发者支持更新仓库代码和浏览仓库成员列表；
   - 浏览者支持浏览、评论仓库。

2. **IP白名单控制**
   - IP白名单是对IP范围开设的白名单，通过设置IP白名单能极大增强您的仓库的安全性。
   - 只有在IP白名单范围内的IP才可以访问仓库。除此之外其他IP发起的访问将被拒绝。

- IP白名单包括租户级IP白名单和仓库级IP白名单，并可配置优先级。

关于IP白名单的详细配置方法，请参见**配置IP白名单**。

3. **锁定仓库**

   为防止任何人破坏即将发布版本的代码仓库，管理员可以锁定仓库，在锁定仓库后，任何人都无法向任何分支提交代码（包括管理员本人）。

   关于锁定仓库的详细操作方法，请参见**锁定仓库**。

4. **保护分支管理**

   分支保护，可防止分支被其他人提交或误删。

   - 保证分支的安全性，允许开发人员使用合并请求合入代码。
   - 阻止管理者以外的人推送代码。
   - 阻止任何人强行推送到此分支。
   - 阻止任何人删除此分支。

   关于保护分支的详细配置方法，请参见**配置保护分支**。

5. **运维SOD**

   为规范开发、测试、发布上线全流程运维脚本（包含脚本开发、代码检视、手动测试、集成验收、发布审核、脚本上线、版本管理等），推行和加强标准化作业的管理，保证流程合规、安全合规、质量合规。

6. **防护墙和VPC隔离**

   CodeArts Repo通过防护墙和VPC隔离支持租户间网络和资源隔离。

6.3 数据保护技术

CodeArts Repo通过多种手段保护数据安全。

数据保护手段	简要说明	详细介绍
传输加密（HTTPS）	通过在云端对托管在CodeArts Repo的代码库进行落盘加密，可以有效避免数据拥有者之外的人接触到用户的明文数据，避免数据在云端发生泄露。同时，代码加密过程对用户完全透明，用户可以使用任意官方Git端来访问CodeArts Repo上的代码仓库。	-
密钥管理	通过SSH密钥和部署密钥管理，确保请求发起是请求发起方，让用户只能浏览被授权的数据，保证数据安全。	关于SSH密钥详细介绍及获取方式，请参见**SSH密钥**。

数据保护手段	简要说明	详细介绍
git-crypt加密传输与存储	git-crypt是一款第三方开源软件，可以用于对Git仓库中的文件进行透明化的加密和解密。	其可对指定文件、指定文件类型等进行加密存储，开发者可以将加密文件（如机密信息或敏感数据）与可共享的代码存储在同一个仓库中，并如同普通仓库一样被拉取和推送，只有持有对应文件密钥的人才能查看到加密文件的内容，但并不会限制参与者对非加密文件读写。关于git-crypt加密传输与存储详细介绍及获取方式，请参见**git-crypt加密**。
敏感数据匿名和高价值数据加密	CodeArts Repo在利用统一、准确的数据支撑应用程序和服务的同时充分保障了数据安全性和隐私性。	日志和数据库中无可避免有一些敏感数据，包含但不限于密钥，帐号信息等等。为防止敏感数据泄露造成安全问题，我们会把这些数据进行匿名或者加密处理，其原理是哈希函数，是对一段信息产生信息摘要，以防止被篡改。
防DDOS工具	DDoS高防（Anti-DDoS）是防护DDoS攻击的工具。当您的互联网服务器遭受大流量的DDos攻击时，DDoS高防可以保护其应用服务持续可用。	DDoS高防支持通过DNS解析和IP直接指向两种引流方式，实现网站域名和业务端口的接入防护。根据您在DDoS高防中为业务配置的转发规则，DDoS高防将业务的DNS域名解析或业务IP指向DDoS高防实例IP或CNAME地址进行引流。 来自公网的访问流量都将优先经过高防机房，恶意攻击流量将在高防流量清洗中心进行清洗过滤，正常的访问流量通过端口协议转发的方式返回给源站服务器，从而保障源站服务器的稳定访问。
流量限制	流量限制可以用来限制用户在给定时间内HTTP请求的数量，流量限制用来保护上游应用服务器不被同时太多用户请求所压垮。	CodeArts Repo的主要使用Nginx流控和APIGW流控。Nginx的流量限制使用漏桶算法，该算法在通讯和分组交换计算机网络中广泛使用，用以处理带宽有限时的突发情况。APIGW流控可限制单位时间内API的被调用次数，保护后端服务，提供持续稳定的服务。
容灾备份	容灾备份不仅保证数据不丢失，还要保证在服务器宕机后接管服务器的业务，保证业务连续性。保障用户可以不间断的使用应用服务，让用户的服务请求能够持续运行，保证信息系统提供的服务完整、可靠、一致。	-

数据保护手段	简要说明	详细介绍
Hash分片存储	Hash分片存储，即通过数据分片提高隐私性和私密性，就是按照一定的规则，将数据集划分成相互独立正交的数据子集。然后数据被随机分散到多个节点中，没有任何一个节点可以访问完整的数据，它们只包含数据的某一部分。	-
水印	为防止未经授权拍照、截图或其他手段随意传播公司核心资产，可以开启水印设置。	关于水印的详细设置方法，请参见**设置水印**。
备份	仓库备份操作保障代码安全，防止他人误删除，分为两种备份形式。 • 将仓库备份到华为云的其它区域。 • 将仓库备份到您本地计算机。	关于备份仓库的详细操作方法，请参见**备份仓库**。

6.4 审计与日志

审计

云审计服务（Cloud Trace Service，CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

用户开通云审计服务并创建和配置追踪器后，CTS可记录CodeArts Repo的管理事件和数据事件用于审计。

CTS的详细介绍和开通配置方法，请参见**CTS快速入门**。

日志

- **云日志**

云日志服务（Log Tank Service）提供一站式日志采集、秒级搜索、海量存储、结构化处理、转储和可视化图表等功能，满足应用运维、网络日志可视化分析和运营分析等应用场景。

出于分析问题的目的，CodeArts Repo将系统运行的日志实时记录到LTS，并保存3天。

基于服务器、数据库等的日志进行监控，对触发监控规则的日志信息通过短信和邮件进行告警，确保现网故障和隐患能第一时间被发现并进行有效处理，保证用户的业务正常运转，做到问题的及时发现和处理，最大程度减少对用户业务的影响。

- **操作日志**

操作日志旨在记录代码仓的所有行为活动，相关操作人员和时间点，帮助管理员和仓库所有者监督和回溯代码仓的行为活动。

关于操作日志的详细查看方法，请参见**查看操作日志**。

6.5 监控安全风险

WAF 应用防护系统

CodeArts Repo对接WAF应用防护系统。Web应用防护系统也称为网站应用级入侵防御系统。

WAF通过对HTTP(S)请求进行检测，识别并阻断SQL注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护Web服务安全稳定。

WAF支持云模式、独享模式和ELB模式三种部署模式。

主机围栏

主机围栏可分别对PC设备接入设置、IP地址列表、PC设备标识列表进行安全围栏设置。

OS 加固和异常侦测

OS规范化脚本分为两个脚本，检查脚本（ osstdchk.py ）和修复脚本（ osstdfix.py ）。OS加固需根据华为云OS加固标准进行加固。

6.6 安全运维

变更作业流程

通过脚本在平台进行现网变更，避免在服务器控制台直接操作引发现网故障，并且执行平台操作需符合1+1 check流程，一人实施，另外一人监控和检查，保证流程合规、安全合规、质量合规。

提权操作的控制

依据风险分层分级和权限SOD原则，对权限以及授权过程进行控制。当遇到普通业务告警，需遵循高危和黑名单命令控制，即当进行变更操作时可对其中的命令进行实时监控，并且可通过配置规则对命令危险程度进行等级划分，若检测出高危和黑名单命令，系统会提供实时告警通知，避免违规操作造成业务中断。当遇到紧急业务告警时，提权需遵守规定，确保安全与效率的均衡。

变更操作的审视

变更实施前需进行申请、风险审核、专家组评估等流程。

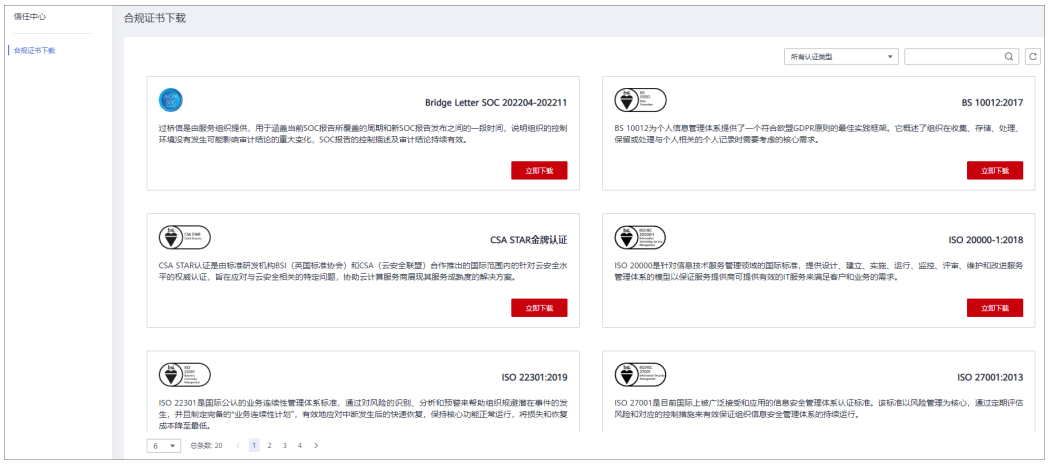
变更实施过程中的每一步操作都必须检查、验证及监控业务情况，检查范围包括变更服务、周边服务及全局的监控告警、拨测及流量变化等，避免出现人为变更导致现网故障。

6.7 认证证书

合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行**申请下载**合规资质证书。

图 6-2 合规证书下载



资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看**资源中心**。

图 6-3 资源中心

7 约束与限制

本节介绍了代码托管中的限制，如下表所示。

表 7-1 使用限制说明

指标类型	指标项	限制说明
浏览器	类型	目前适配的主流浏览器类型包括： ● Chrome ● IE10以上 ● Microsoft Edge ● Firefox ● Safari 推荐使用Chrome、Microsoft Edge浏览器，效果会更好。
分辨率	分辨率大小	推荐使用1920*1080及以上。
单个仓库规格	单文件上传大小限制（评论中上传附件）	<=50MB。
	单文件上传大小限制（代码页签中上传文件）	<=10MB。
	单文件推送大小限制（本地）	<=200MB。
	在线修改代码，单次保存行数限制	<=5000行。

指标类型	指标项	限制说明
	仓库容量（超出容量限制会导致仓库部分功能无法使用，如代码无法上传） **说明** 单仓容量不包括LFS容量，仓库总容量 = 单仓容量* 单仓个数 +LFS容量 ，LFS大文件是通过git客户端上传，上传的单文件容量最大为2GB。	<=2GB。

说明

当您处于以下情况时，会受到的影响：

- **仓库容量超出限制**：超出容量限制会导致仓库部分功能无法使用，如新建/编辑文件、新建目录、新建子模块、新建分支/tag、上传文件、解决代码冲突、合入合并请求、Git客户端推送等。仓库容量正常后，系统启动定时任务恢复仓库状态。
- **关闭代码托管服务：**您不可进入仓库，界面并提示需开通服务，开启代码托管服务后，恢复仓库状态。关闭代码托管服务超过30天，系统自动删除仓库，不可恢复。