

政企自服务管理

产品介绍

文档版本 01
发布日期 2025-09-30



版权所有 © 华为云计算技术有限公司 2025。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI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。

目 录

1 什么是政企自服务管理.....1

2 产品优势.....2

3 应用场景.....3

4 功能介绍.....4

5 安全.....5

5.1 责任共担.....5

5.2 数据保护技术.....6

6 权限管理.....9

7 约束与限制.....11

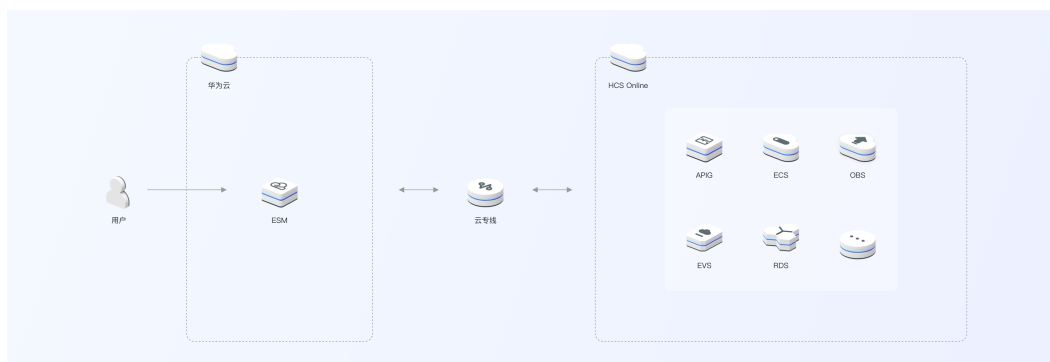
8 修订记录.....12

1 什么是政企自服务管理

政企自服务管理（Enterprise Self-Service Management，ESM）是提供在线云平台运营自管理的服务，ESM构建轻量化在线运营管理服务实现与华为专属云联动，提升客户对专属云平台自助运营管理能力。提供全面、多维度站点状态展示与分析能力，助力客户全面掌握云平台健康状态。

产品架构

图 1-1 ESM 产品架构



访问方式

ESM提供了Web化的服务管理平台，即管理控制台管理方式。

如果用户已注册华为账号并实名认证，可直接登录管理控制台，从主页选择或搜索“政企自服务管理 ESM”访问ESM服务。如果未注册，请先[注册](#)华为账号并[实名认证](#)。

2 产品优势

- 看的多、看的细
支持多业务黄金指标（运维分析数据客户呈现）、安全态势展现，让客户对云资源状态有全面、多维度的掌握，及时有效应对风险挑战。
- 管得住、可介入
支持账户管理、对账单管理、审批、审计等，客户管云团队可以对云资源使用进行自助有效的管理。
- 用得好、可持续
版本更新推送，自动化升级、安全策略升级，使客户的云资源处于最佳状态。

3 应用场景

ESM服务适用于以下场景：

- 内部管理：集团内公司面向子公司和分支机构的内部运营，要求提供本地的账号管理、配额管理、提供计量话单API等功能。
- 面向ToB的运营场景：行业云和政务云类项目面向ToB的运营诉求，提供基于HCSO场景的完整的运营平台与门户。

核心价值：政企自服务管理为专属云用户提供资源池信息大屏可视以及大屏数据开放API共享能力、同时满足租户账号开销户、配额管理运营管理能力。

4 功能介绍

平台管理

支持客户自助开销户，实现客户对云平台的自助管理。

运营管理

对云服务使用配额和计量话单进行管理，让客户实时感知平台整体运行情况、有效实现对平台资源的管控。

全景可视

提供标准数据大屏，可直观监控资源、租户、服务、应用、告警等数据，开放标准 API，支持与客户第三方管理平台对接，实现企业数字化运营。

5 安全

5.1 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。

与传统的本地数据中心相比，云计算的运营方和使用方分离，提供了更好的灵活性和控制力，有效降低了客户的运营负担。正因如此，云的安全性无法由一方完全承担，云安全工作需要华为云与您共同努力，如[图5-1](#)所示。

- **华为云：**无论在任何云服务类别下，华为云都会承担基础设施的安全责任，包括安全性、合规性。该基础设施由华为云提供的物理数据中心（计算、存储、网络等）、虚拟化平台及云服务组成。在PaaS、SaaS场景下，华为云也会基于控制原则承担所提供服务或组件的安全配置、漏洞修复、安全防护和入侵检测等职责。
- **客户：**无论在任何云服务类别下，客户数据资产的所有权和控制权都不会转移。在未经授权的情况，华为云承诺不触碰客户数据，客户的内容数据、身份和权限都需要客户自身看护，这包括确保云上内容的合法合规，使用安全的凭证（如强口令、多因子认证）并妥善管理，同时监控内容安全事件和账号异常行为并及时响应。

图 5-1 华为云安全责任共担模型



云安全责任基于控制权，以可见、可用作前提。在客户上云的过程中，资产（例如设备、硬件、软件、介质、虚拟机、操作系统、数据等）由客户完全控制向客户与华为云共同控制转变，这也就意味着客户需要承担的责任取决于客户所选取的云服务。如图5-1所示，客户可以基于自身的业务需求选择不同的云服务类别（例如IaaS、PaaS、SaaS服务）。不同的云服务类别中，每个组件的控制权不同，这也导致了华为云与客户的责任关系不同。

- 在On-prem场景下，由于客户享有对硬件、软件和数据等资产的全部控制权，因此客户应当对所有组件的安全性负责。
- 在IaaS场景下，客户控制着除基础设施外的所有组件，因此客户需要做好除基础设施外的所有组件的安全工作，例如应用自身的合法合规性、开发设计安全，以及相关组件（如中间件、数据库和操作系统）的漏洞修复、配置安全、安全防护方案等。
- 在PaaS场景下，客户除了对自身部署的应用负责，也要做好自身控制的中间件、数据库、网络控制的安全配置和策略工作。
- 在SaaS场景下，客户对客户内容、账号和权限具有控制权，客户需要做好自身内容的保护以及合法合规、账号和权限的配置和保护等。

5.2 数据保护技术

为了确保您的个人数据（例如用户名、密码、手机号码等）不被未经过认证、授权的实体或者个人获取，ESM通过多种数据保护手段和特性，保障数据的安全可靠。

收集范围

通过ESM工单收集及产生的个人数据参见[表 个人数据范围列表](#)。

表 5-1 个人数据范围列表

类型	收集方式	使用目的	是否可以修改	是否必须	生命周期
用户名	注册华为云账号时提供	用于通知工单处理进展	是	是	用户帐号注销，会被清除
IP	使用服务时	记录审计日志	否	是	日志清空时删除
工单信息	在创建工单以及留言页面提交的信息，包括描述、留言、上传日志截图等文件	- 在创建工单以及留言页面提交的信息，在处理过程中服务人员要求提供的信息以更快更准确的定位处理问题 - 提交时请注意不要在工单描述、留言、日志文件等地方提交个人敏感数据，比如密码、手机号等	否	是	工单信息是工单处理的基本必要信息，不包括个人敏感数据，出于质检、审计等目的，数据将长期保存
邮箱	- 在创建工单页面提供的联系邮箱 - 注册华为云账号时提供的邮箱	- 如果希望获取工单进展通知时需要填写 - 注册邮箱仅作为紧急联系方式，工单处理、回访等会优先联系创建工单提交的邮箱	是	是/否（邮箱与手机号收集方式至少必须一个）	- 在提单页面新认证的邮箱有效期为90天，到期自动清除 - 华为云帐号注销后，注册联系邮箱、手机号等信息会清除

类型	收集方式	使用目的	是否可以修改	是否必须	生命周期
手机号	- 在创建工单页面提供的联系手机号 - 注册华为云账号时提供的手机号	- 如果希望获取工单进展通知时需要填写 - 注册手机号仅作为紧急联系方式，工单处理、回访等会优先联系创建工单提交的手机号	是	是/否（手机号与邮箱收集方式至少必须一个）	

存储方式

工单系统通过加密算法对以下用户个人敏感数据加密后进行存储。

- 邮箱、手机、授权信息：加密存储。
- 工单信息：不属于个人敏感数据，明文存储。

访问权限控制

用户个人数据通过加密后存储在工单数据库中，数据库的访问需要通过白名单的认证与授权。

API 接口限制

用户调用API接口时，需要使用IAM Token进行认证。

6 权限管理

ESM 权限

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

权限根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。多数细粒度策略以API接口为粒度进行权限拆分，ESM支持的API授权项请参见ESM策略及授权项说明。

如表6-1所示为ESM的所有系统策略。

表 6-1 ESM 系统权限

策略名称	描述	策略类型	策略使用建议
ESM FullAccess	拥有ESM管理权限，可以使用ESM所有功能。	系统策略	建议对进行开销户的管理员用户分配该策略。
ESM ReadOnly Access	拥有ESM只读权限，不可进行修改操作。	系统策略	建议对使用大屏可视的管理员用户分配该策略。

授权项说明

ESM当前所支持的系统策略操作与API相对应，授权项内容请参见表6-2。授权项列表说明如下：

- 权限：允许或拒绝对指定资源在特定条件下进行某项操作。
- 授权项：系统策略中支持的Action。

表 6-2 授权项说明

所属策略	权限	授权项（ Action ）
ESM FullAccess	HCSO局点管理	esm:hcsso:get esm:hcsso:list esm:hcsso:update
	HCSO租户管理	esm:hcssoTenant:create esm:hcssoTenant:delete esm:hcssoTenant:get esm:hcssoTenant:list esm:hcssoTenant:update esm:hcssoTenantOwnerUser:create esm:hcssoTenantOwnerUser:update
	HCSO project查询	esm:hcssoProject:list
	配额管理权限	esm:hcssoQuota:get esm:hcssoQuota:update
	可视化查看	esm:hcssoDashboard:use
	告警通知管理	esm:hcssoDashboard:create esm:hcssoDashboard:get esm:hcssoDashboard:delete esm:hcssoDashboard:update esm:hcssoDashboard:list
	更新Logo	esm:DashboardLogo:put
ESM ReadOnlyAccess	HCSO局点只读	esm:hcsso:get esm:hcsso:list
	HCSO租户只读	esm:hcssoTenant:get esm:hcssoTenant:list
	HCSO project查询	esm:hcssoProject:list
	配额只读	esm:hcssoQuota:get
	可视化查看	esm:hcssoDashboard:use
	告警通知只读	esm:hcssoDashboard:get esm:hcssoDashboard:list

7 约束与限制

政企自服务管理ESM目前处于商用阶段，网络安全大屏功能暂未提供，敬请期待！

8 修订记录

发布日期	修订记录
2025-03-30	第六次正式发布。
2024-11-30	第五次正式发布。
2024-07-30	第四次正式发布。
2024-04-30	第三次正式发布。
2023-11-30	第二次正式发布。
2023-10-30	第一次正式发布。