

交换数据空间

产品介绍

文档版本 02
发布日期 2025-01-21



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。

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 图解交换数据空间 | 1 |
| 2 什么是交换数据空间 | 3 |
| 3 产品优势 | 7 |
| 3.1 交换数据空间产品优势 | 7 |
| 3.2 DMAP 数小二产品优势 | 7 |
| 4 应用场景 | 9 |
| 4.1 交换数据空间应用场景 | 9 |
| 4.2 DMAP 数小二应用场景 | 10 |
| 5 安全 | 12 |
| 5.1 身份认证与访问控制 | 12 |
| 5.2 数据保护技术 | 12 |
| 5.3 服务韧性 | 12 |
| 6 权限管理 | 14 |
| 7 约束与限制 | 17 |
| 8 与其他云服务的关系 | 18 |
| 9 基本概念 | 19 |

1 图解交换数据空间

2 什么是交换数据空间

交换数据空间

交换数据空间（Exchange Data Space，简称EDS）面向数据要素流通场景，提供数据交换过程中的安全保护技术能力，如数据使用策略、日志审计、数据市场等。您可以选择相应的安全策略，让数据在提供方和消费方交换过程中，按照对应策略的约束使用数据，同时EDS提供相应的日志审计能力，帮助您了解数据在交换流转中的操作过程。

产品架构

EDS产品架构如[图2-1](#)所示。

图 2-1 产品架构



产品模块说明：

- 数据市场**
 提供数据搜索、资产标注、需求匹配、合约协商、数据订阅等功能，帮助消费方快速、高效地找到有价值的数。
- 认证中心**
 基于规范的认证标准，对数据交换各方的身份和资质认证，建立一个多方信任的生态环境。
- 清算中心**
 对数据交换过程的操作记录日志，实现日志管理能力，提供全流程可信、可视的日志审计追溯服务，支持提供方查证追溯，也能让消费方免证清白，同时为第三方监管提供相应的审计信息。
- 使用控制中心**
 EDS的核心模块，对每次交换的数据进行使用策略制定，用来对交换后的数据使用进行安全合规的控制。
- 数据连接器**
 EDS的核心模块，提供数据集成、计算和消费能力，通过连接器实现数据提供方和数据消费方之间数据的流通和可控使用。
- 数据传输**
 数据连接器中的传输模块，用来将数据从数据提供方传输到数据消费方，并提供通道加密的能力。

- **数据存储**
数据连接器中的存储模块，用来存储在数据空间中交换的数据。
- **数据分析应用**
数据连接器中的应用模块，主要是在数据消费方的连接器中。用来对交换的数据进行分析处理，实现对数据的消费使用。数据分析应用在使用数据的过程中遵循使用策略的控制，保障对数据主权的安全保护。
- **数据使用控制**
数据连接器中的核心模块，用来执行使用策略，实现对交换数据在使用过程中的保护。

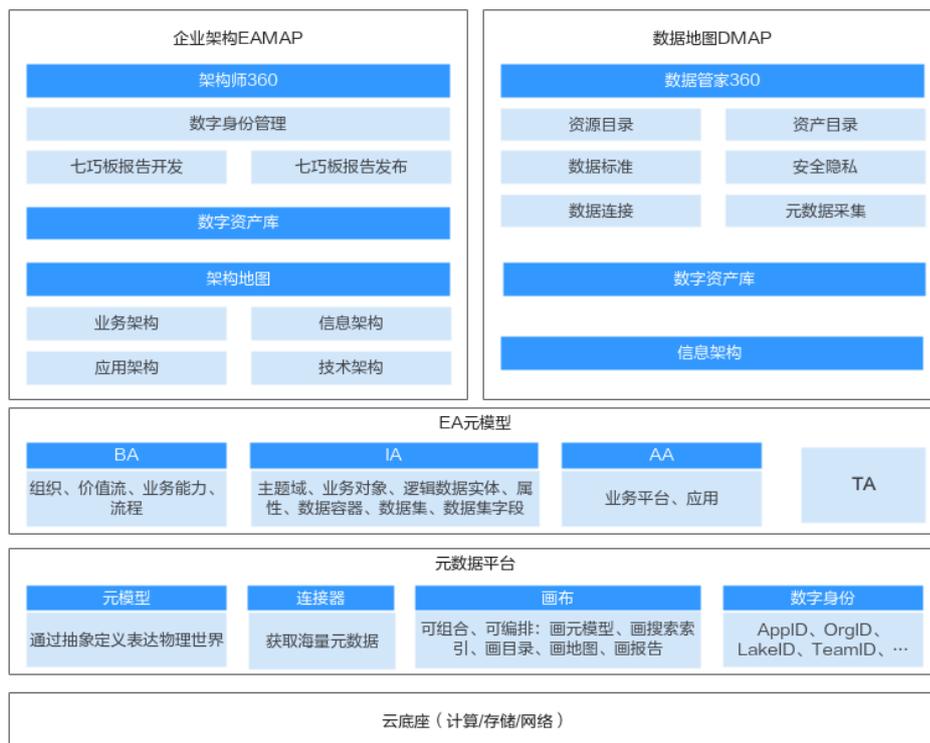
DMAP 数小二

DMAP数小二是承载《华为数字化转型之道》、《华为数据之道》理论精华，从业务、数据、应用、技术视角对企业核心信息进行运营和管理的平台，是对企业数字化世界的描述，也是企业数字化资产的入口，致力于帮助政企组织开展企业数字化资产的正向循环和全生命周期运营，最终通过平台预制数字化模板和自助构建模式，助力企业在数字化时代实现高效运营、加速转型。

产品架构

DMAP数小二产品架构如图2-2所示。

图 2-2 产品架构



产品模块说明：

- **架构师360**
提供给企业架构师（业务架构师、应用架构师、数据架构师）的管理工具，实现对基于EA元模型的数字身份、数字化报告模板的管理。

- **数字资产库**
数字资产的综合查询库，支持架构资产一键式搜索，通过丰富的过滤条件，包括资产类型、密级两大类，可快捷直达所需资产。
- **架构地图**
提供给普通消费者查阅遵从TOGAF 10定义的架构资产（架构制品Artifact），包括目录Catalog、地图Map、矩阵Matrices、图表Diagram四类制品，将数字资产库中的资产进行可视化呈现，使数字资产支撑管理决策。
- **七巧板报告**
七巧板报告的开放市场，用于企业员工查看数字化报告，实现团队内共享使用。内置丰富的七巧板报告模板，覆盖主要企业架构制品。利用元模型技术分钟级完成七巧板报告的开发。
- **数据管家360**
提供给数据管家和数据Owner的管理工具，实现对数据源、技术元数据采集、信息架构、数据标准等的管理。
- **运营中心**
集中查看支撑运营根技术的模块，内含元模型中心，从信息架构、业务架构、应用架构三大层面感知元模型的驱动力。
- **EA元模型**
基于企业架构管理优秀经验孵化，遵从CWM/MOF/TOGAF国际标准。元模型中涵盖数据资产管理相关的能够反应物理世界运作的实体，定义BA、AA、IA、TA相关核心实体和特征，支持数字化能力运营。
- **元数据平台**
DMAP数小二的技术引擎平台，以ABM应用业务模型为载体，包含元模型、连接器、画布、数字身份等根技术，实现元数据驱动应用开发，保障企业架构资产的高质量运营。

3 产品优势

3.1 交换数据空间产品优势

可信：构造多方信任的生态环境

通过与云认证打通、发放证书等措施，对企业组织、角色及技术组件进行可信认证，建立统一的信任机制，实现参与方身份与平台环境可信任。

可控：打造可组合的使用控制策略

平台提供“有效期限、查看次数、是否下载”等多种使用控制策略的制定、管理和策略执行能力。在数据使用过程中基于策略做出相应的控制，确保在数据主权可控的基础上合规使用数据。

可证：安全审计追溯

提供全流程可信、可视的审计追溯服务，支持提供方查证追溯，也能让消费者免证清白，同时开放接口为第三方监管提供相应的审计信息。

3.2 DMAP 数小二产品优势

华为 EA5.0 优秀管理实践经验外溢，助力企业架构数字化敏捷管理

- 遵循华为EA5.0优秀管理实践，沉淀标准架构制品，实现元数据驱动数字化应用开发
- 参照华为数字化转型框架，借助优秀实践沉淀和方法论，以经验提效率
- 搭建战略到变革实施落地的桥梁，以数字化手段提升企业架构管理协作效率

EA 标准元模型内置，开箱即用，实现物理世界到数字世界的精准刻画

- 遵从TOGAF国际标准及ADM开发方法论，高度标准化，以元模型驱动海量数据应用的生成
- 元数据驱动，基于元模型设计搜索、卡片、目录，满足不同客户的个性化需求

- 基于EA元模型，便于开展数字身份管理，成为数字能力运营的基石
- 元模型支持个性化拓展，可根据企业自身实践按需拓展实体、关系、特征

多类型连接器加持，提升对海量元数据的采集力，与数据源创建广泛和深度的连接

- 内置丰富元数据连接器，快速采集元数据资产
- 支持多源异构数据资产采集，准实时感知技术元数据变动，提升业务实时性
- 支持连接器开放框架，使能伙伴快速开发第三方连接器

数字化报告分钟级构建，数字化成果实时可视，精准辅助决策

- 元模型驱动40+数字化报告模板，开箱即用，通过元数据注册分钟级无码化构建CXO报告
- 支持涂鸦、EA报告等画布模式，可组合可编排，通过拖拽方式快速实现自定义的数字化报告页面开发
- 实现架构资产数字化，使企业架构建得明白、用得清楚，满足业务人员需求

元数据更多维、地图更智能，加速业务人员用数效率

- 元数据360度刻画，包含技术元数据、业务元数据、管理元数据、操作元数据、质量/协同元数据等6类
- 构建可搜索、可理解、可共享、可自助分析的数据资产地图
- 数据按密级授权，确保数据安全可控，轻松查找及请求访问数据
- 支持分钟级感知数据模型变化，元数据信息链辅助数据应用的影响分析

4 应用场景

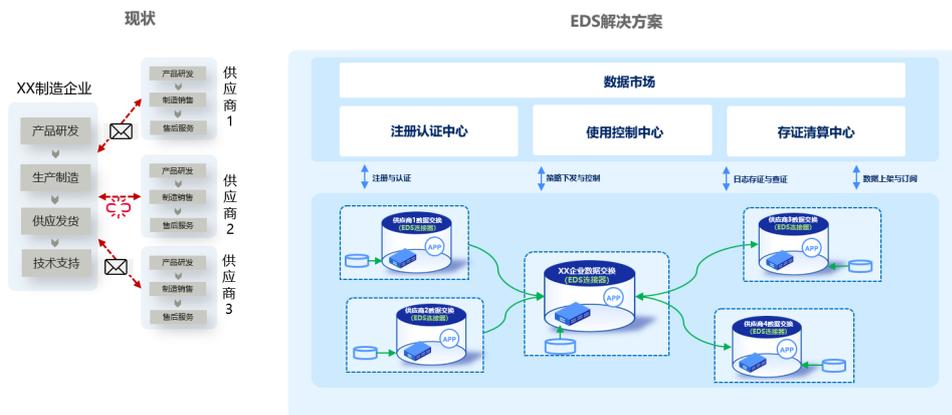
4.1 交换数据空间应用场景

企业上下游业务协同

场景描述

企业与相关的上下游伙伴企业如供应商、研发和服务伙伴之间的业务协同如研发协同，上下游供应链质量追溯等，需要双方交换相关的数据。对数据交换时的传输，需确保使用上的安全，确保数据交换的安全可控，实现企业安全放心的交换数据。

图 4-1 企业上下游业务协同场景



现状问题

该场景缺少互信关系的保障方案和机制：当前大部分还是以人工邮件申请传递，安全难以得到保障，且很多业务协同过程中涉及到敏感数据如研发设计文档、产品质量数据等，传输也相对很谨慎，通常会形成数据断点，业务协同效率差。

方案收益

EDS方案实现了数据交换过程的安全保护机制，为企业带来的价值：增强了生态之间的互信，数据合规使用充分发挥了数据价值，提升了企业内外部业务协同的效率。

行业产业链协同

场景描述

针对产业云/赋能云，行业运营平台等场景，细分行业链。企业进行产业协同，通过数据交换实现完整的业务创新闭环。例如：在制造加工类行业工艺设计场景中，制造设备厂家、工艺设计师和客户三方围绕工艺设计会进行产品设计模型、加工设备模型以及工艺包等数据的交换，其中部分数据在使用时需要安全保护。

现状问题

当前工艺设计和优化，主要还是通过制造加工企业雇佣工艺师，或者通过外包的模式实现。通过合同保障来约束数据的合规使用以及权益保护。工艺经验难以得到沉淀，不利于行业产业链能力发展。

方案收益

EDS提供数据安全交换能力，协同行业运营平台形成联合方案，实现安全数据流通底座，通过产业云/赋能云模式，帮助行业各类上下游公司实现产业链协同。

4.2 DMAP 数小二应用场景

数据资产运营

现状问题

- 组织内存在数据不可见、查找困难、标准不统一，无法理解、权限管控难等问题。
- 数据资源无法有效转化成数据资产，业务与IT之间存在巨大屏障，阻碍数据价值的具体发挥。

方案收益

- 实现数据资产的全域盘点，支持语义搜索，帮助用户一键查找所需。
- 支持360度资产刻画，实现数据集、逻辑数据实体、隐私密级的详情查看，帮助用户全面理解数据，洞悉数据资产的流通全局，提升可信度。
- 基于AppID开展数据隐私及密级管理，加强对数据资产的安全可控。

企业架构资产运营

现状问题

- 组织内企业架构资产散落在各处，多数以非结构化方式保存，查找困难，费时费力。
- 架构视图和符号没有统一标准和一致规范，会出现表达信息不一致的问题，导致理解和沟通有偏差。

方案收益

- 遵循TOGAF国际标准及华为EA5.0实践经验，形成标准架构制品，实现企业架构资产的有序梳理。
- 架构资产在线化管理，一键搜索获取，帮助对齐语言，最大化提升协同效率。

数字化报告可视化

现状问题

- 业务、应用、数据和技术架构的变更通过线下方式进行，没有通过统一的系统来发布和承载。
- 企业的数字化转型过程中的大量投入及工作成果无法快速准确、直观的体现出来。

方案收益

- 元模型驱动40+数字化报告模板生成，开箱即用，分钟级构建数字化报告。
- 基于AppID开发的数字化报告，让CXO洞察数字化变革进展。
- EA元模型，将数字资产像七巧板一样自由组合，形成利益相关人关心的、多维度的、能辅助决策的数字化报告。

应用架构规划与集成开发一体化

现状问题

企业架构管理过程中，因无统一语言与标准，4A架构未形成一体化有机体，各个架构部分分头工作，业务/信息架构与应用/技术架构之间存在断层，架构集成关系不好管，无法实现从业务到IT。

方案收益

DMAP数小二应用架构有效集成应用平台AppStage，打通与AppStage的应用开发体验，实现一体化应用设计到开发，帮助快速高效提升应用开发及管理效率。

5 安全

5.1 身份认证与访问控制

- 身份认证：EDS与IAM打通，对EDS数据空间，企业租户可以使用华为云用户名与密码登录，实现租户的认证与鉴权，未授权的不能访问。
- 访问控制：企业中的员工可以使用华为云租户下面的子用户，EDS支持在数据空间中对子用户进行角色管理，并对角色设置数据空间中的数据访问权限。

5.2 数据保护技术

EDS通过数据加密保护手段，保护数据空间中的数据安全，如表5-1所示。

表 5-1 交换数据空间的数据保护手段

| 数据保护手段 | 简要说明 |
|-----------------|--|
| 传输加密 (HTTPS) | EDS数据空间之间数据传输接口支持HTTPS传输协议，保障数据传输的安全性。 |

5.3 服务韧性

EDS提供了3级可靠性架构，通过双AZ容灾、AZ内集群容灾、数据容灾技术方案，保障服务的持久性与可靠性。

EDS可靠性方案，如表5-2所示。

表 5-2 交换数据空间可靠性架构

| 可靠性方案 | 简要说明 |
|-------|---------------------------------|
| 跨AZ容灾 | EDS实现2AZ双活，一个AZ异常时不影响云服务持续提供服务。 |

| 可靠性方案 | 简要说明 |
|---------|---|
| AZ内集群容灾 | EDS通过集群提供服务，集群中每个微服务都有多个实例，当一个或部分实例异常时，其他实例可以持续提供服务。 |
| 数据容灾 | EDS内部数据存储于RDS服务中，RDS实现了AZ容灾方案，数据持续会同步到容灾站点。当生产站点的RDS异常后，容灾站点可以接管业务，保障云服务持续运行。 |

6 权限管理

如果您需要对华为云上购买的EDS资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在华为云账号中给员工创建IAM用户，并授权控制他们对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有EDS的使用权限，但是不希望他们拥有删除EDS资源的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用EDS，但是不允许删除EDS资源的权限，控制他们对EDS资源的使用范围。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用EDS服务的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。关于IAM的详细介绍，请参见[IAM产品介绍](#)。

EDS 权限

默认情况下，管理员创建的IAM用户没有任何权限，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。

EDS部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域（如华北-北京1）对应的项目（cn-north-1）中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问EDS时，需要先切换至授权区域。

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。由于华为云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。例如：针对EDS服务，管理员能够控制IAM用户仅能对交换数据空间进行指定的管理操作。

如表6-1所示，包括了EDS的所有系统权限。

表 6-1 EDS 系统权限

| 策略名称 | 描述 | 策略类别 | 策略内容 |
|--------------------|--------------------------------------|------|--|
| EDS FullAccess | 交换数据空间服务所有执行权限，拥有该权限的用户可以执行所有操作。 | 系统策略 | EDS FullAccess策略内容 |
| EDS ReadOnlyAccess | 交换数据空间的只读权限，拥有该权限的用户仅能查看当前实例下连接器的数量。 | 系统策略 | EDS ReadOnlyAccess策略内容 |

表6-2列出了EDS常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 6-2 常用操作与系统权限的关系

| 操作 | EDS FullAccess | EDS ReadOnlyAccess |
|--------------|----------------|--------------------|
| 创建交换数据空间实例 | √ | x |
| 删除交换数据空间实例 | √ | x |
| 申请加入交换数据空间实例 | √ | x |
| 申请开通连接器 | √ | x |
| 申请加入连接器 | √ | x |
| 删除连接器 | √ | x |
| 查询当前实例下所有连接器 | √ | √ |
| 创建DMAP实例 | √ | x |
| 升级DMAP实例规格 | √ | x |
| 查询已开通的DMAP实例 | √ | √ |

相关链接

- [IAM产品介绍](#)
- 创建用户组、用户并授予EDS权限请参考：[创建用户并授权使用EDS](#)
- 管理账号下子用户对连接器的权限请参考：[用户管理](#)

EDS FullAccess 策略内容

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
```

```
    "Action": [
      "eds:*"
    ]
  }
]
```

EDS ReadOnlyAccess 策略内容

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "eds:connector:list"
      ]
    }
  ]
}
```

7 约束与限制

交换数据空间的使用限制如下：

- 每个租户交换数据空间下，创建子用户数不能超过50个。
- 连接器之间传输的单个非结构文件大小不超过20MB。

DMAP数小二的使用限制如下：

- 通过Excel导入架构资产时单个文件大小不超过10MB。
- 通过Excel导入架构资产时单个工作表的最大行数不超过20000，单个工作表的最大列数不超过1000，单个文件最大页签为400。

8 与其他云服务的关系

统一身份认证服务

EDS使用统一身份认证服务（Identity and Access Management，简称IAM），实现认证和鉴权功能。

云审计服务

使用云审计服务（Cloud Trace Service，简称CTS），审计用户在管理控制台页面的操作，可用于检视是否存在非法或越权操作，完善服务安全管理。

应用运维管理

使用应用运维管理（Application Operations Management，简称AOM），实现监控和日志管理功能。

对象存储服务

使用对象存储服务（Object Storage Service，简称OBS），实现数据空间连接器中非结构化交换数据的存储。

云数据库

使用云数据库（RDS for MySQL），实现数据空间连接器中结构化交换数据的存储。

数据集成工具

使用DataArts Studio-DataArts Migration/ROMA Connect FDI，实现数据集成功能。

区块链服务

使用区块链服务（Blockchain Service，简称BCS），实现数据上链的功能，通过对比链上链下的数据来判断链下数据是否被篡改。

组织成员管理

使用组织成员账号（OrgID），提供组织管理、企业成员账号管理。

9 基本概念

连接器 Connector

部署在数据提供方和消费方空间的软件程序，用于实现数据交换，以及过程中的数据使用控制。

数据资源

待交换的数据，由数据提供方提供。

数据 Offer

由数据提供方提供的对待交换数据的元数据描述信息，并上架到共享市场形成资产，供多个消费方进行搜索订阅，共享市场上的这份资产称为数据Offer。

使用控制策略

针对待交换的数据在使用过程中的控制规则，对数据的使用进行保护，策略由数据提供方制定。

认证中心

对数据提供方、数据消费方的连接器Connector进行合法性认证校验，发放数字证书。

审计中心

记录存储数据在提供方与消费方交换过程中的日志，供查询、审计、追溯用。

数据分析应用

运行在连接器Connector中的数据应用，按照数据使用策略的要求进行数据的访问使用。

信息架构

信息架构是以结构化的方式描述在业务运作和管理决策中所需要的各类信息及其关系的一套整体组件规范。信息架构包括数据资产目录、数据标准、企业级数据模型和数据分布四个组件。

数据 Owner

数据Owner是公司数据战略的制定者、数据文化的营造者、数据资产的所有者、数据争议的裁决者、数据质量的保障者和信息架构的决策者，拥有公司数据日常管理的最高决策权。数据Owner又称数据所有者。

数据管家

数据管家是数据Owner的助手，是数据Owner在数据管理方面的具体执行者。

数据资产目录

数据资产目录是企业数据按照业务维度进行分类的一个有序清单。

数字身份

数字身份是一种身份标识方式，具备唯一性，其中包含了与数据相关的某些实体的数字信息以及与其他实体的关系，如：作为数据来源的应用，为其赋予数字身份，即生成应用数字身份——应用ID。

企业架构

依据企业架构标准组织The Open Group的定义，企业架构描述构成企业的要素和要素之间关系，以及用于管控架构设计和演进的原则和指引。

架构制品

架构制品是一个从某个特定视角进行架构描述并具备更细粒度的工作产品。就表现形式来讲，架构制品的内容可以通过目录、矩阵和图这三种方式来表述。通常情况下，一个架构交付物可以包含多个架构制品，而架构制品也可能会出现在多个架构交付物之中。例如：流程分层图、流程视图。