**数据中心 - 系统设计文档**

V1.0.0

张立丹 @ Enlink 数据中心

**目录**

[1. 概述 3](#_Toc530499895)

[1.1. 系统说明 3](#_Toc530499896)

[1.2. 系统模块 3](#_Toc530499897)

[1.3. 系统目标 4](#_Toc530499898)

[2. 数据接入 5](#_Toc530499899)

[2.1. 模块设计 5](#_Toc530499900)

[2.2. 模块说明 5](#_Toc530499901)

[2.2.1. 采集器 5](#_Toc530499902)

[2.2.2. 接收器 6](#_Toc530499903)

[2.2.3. 缓存队列 6](#_Toc530499904)

[2.2.4. 解码器 6](#_Toc530499905)

[3. 数据存储 7](#_Toc530499906)

[3.1. 模块设计 7](#_Toc530499907)

[3.2. 模块说明 7](#_Toc530499908)

[3.2.1. 控制节点 7](#_Toc530499909)

[3.2.2. 数据节点 7](#_Toc530499910)

[3.2.3. 输入/输出代理 8](#_Toc530499911)

[3.2.4. 数据管理 8](#_Toc530499912)

[4. 数据分析 9](#_Toc530499913)

[4.1. 模块设计 9](#_Toc530499914)

[4.2. 模块说明 9](#_Toc530499915)

[4.2.1. 规则脚本 9](#_Toc530499916)

[4.2.2. 规则引擎 10](#_Toc530499917)

[4.2.3. 分析工具 10](#_Toc530499918)

[4.2.4. 机器学习 10](#_Toc530499919)

[5. 系统管理 11](#_Toc530499920)

[5.1. 模块设计 11](#_Toc530499921)

[5.2. 模块说明 11](#_Toc530499922)

[6. 数据可视化 12](#_Toc530499923)

# 概述

本文档描述“数据中心”产品的系统架构设计，帮助或辅导研发人员对“数据中心”产品系统有一个总体的认识。

## 系统说明

本文档主要参考《数据中心 - 产品需求文档》编写，在技术选型上结合了开源社区以及业界“潮流”。根据需求文档描述，本系统具备以下特点：

* **多源数据接入**  
  接入本系统的数据源，包括数据格式、数据内容等均多种多样，无法对原始数据直接进行分析；
* **实时存储分析**  
  接入本系统的数据一般具体有时效性（或实时性），即最近一段时间的数据才具有分析参考价值；
* **自动统计报警**  
  接入本系统的数据，一般的使用需求包括：业务及安全审计、行为或业务分析、业务预测等，这些需求均要求本系统能够提供“自动”功能；
* **灵活数据展示**  
  对于多样化的数据展示，展示层不应依赖任何数据内容，因此需具备高度灵活（可配置）的特点。

## 系统模块

数据中心产品的功能包含了“数据产品”的所有功能，包括：数据采集、数据清洗、数据存储、数据分析、预测及报警等。数据中心系统模块如图1-1所示：

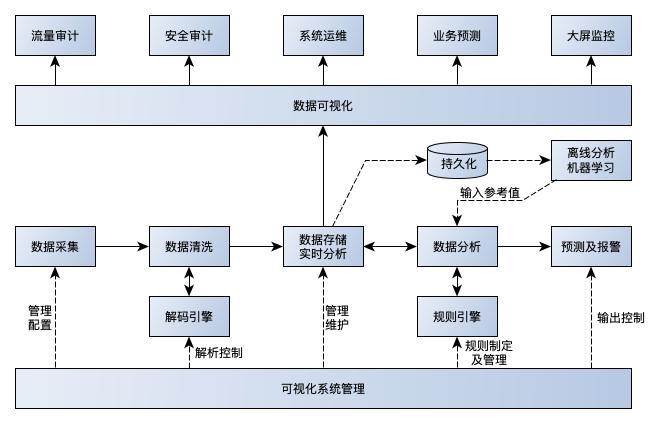


图 1‑1 数据中心系统模块

## 系统目标

数据中心产品面向数据进行设计，属于“纯粹”的数据产品，不依赖于任何系统、业务及行业等。其设计目标包括：

* **适应（兼容）性：多源数据接入**  
  对于不同行业的不同系统所产生的数据，均可接入到数据中心进行分析展示。通过扩展数据采集、解码功能，实现数据的无缝接入。
* **扩展性：数据容量**  
  通过存储模块的横向扩展，实现对“大数据”存储、查询的支持。
* **实时性：快速响应**  
  从数据的产生到生成分析结果，整个过程应控制在较短的时间范围内，以达到数据分析结果的有效性。
* **智能化：自动分析及预警**  
  通过自动调度用户制定的规则，实现自动分析的功能；通过机器学习来发现多维数据之间的相关性。
* **可用性：用户友好**  
  系统中的所有模块及数据处理环节，均提供可视化管理或控制接口，实现系统本身的可控。

本文档后续章节将对系统的每个模块或功能点的设计，进行详细的描述。

# 数据接入

本章节描述数据中心产品中，数据接入（包括数据采集及清洗）功能的详细设计。

## 模块设计

数据接入功能包含数据的采集、过滤、格式化、解码等功能，该功能（或模块）的详细设计如图2-1所示：

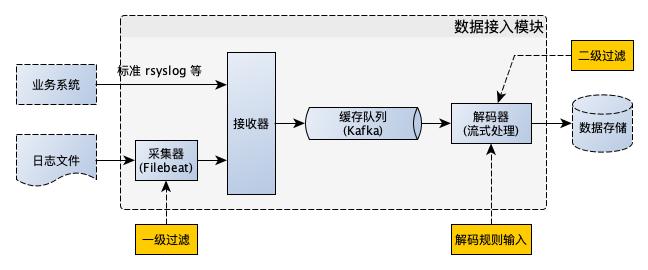


图 2‑1 数据接入模块

其中，可根据数据量的大小来确定是否使用“缓存队列”，当缓存队列不使用时，解码器与接收器能够集成在一起工作；如果使用缓存队列，解码器则能够独立出来，作为“后置”解码器来使用，以提高系统的接入性能。

## 模块说明

本小节描述数据中心产品中，数据接入功能各模块的功能及设计方案。

### 采集器

采集器的主要功能，是将业务系统中的日志文件内容输出到接收器。数据输出之前执行简单的过滤，称为一级过滤。由于采集器运行于目标系统所在机器，不能占用目标机器过多的系统资源（包括内存、CPU、IO等），所有其功能相对简单。

对于日志文件采集而言，数据中心产品中使用开源软件Filebeat作为数据采集器，其具备以下优点：

* **开箱即用**  
  Filebeat的使用、配置文档等全面，直接使用可减少研发工作。
* **轻量级**  
  Filebeat所做的工作特别简单，即将日志文件中的每行数据按增量导出，其占用的系统资源非常少，相对于业务系统而言可以忽略不计。
* **兼容性强**  
  支Filebeat支持多种输入格式及输出方式。

由于Filebeat不具备管理功能，如果要对采集探点进行监控，则需要进行二次开发，且开发难度较大。另外，其配置项较为复杂，学习成功相对较高，不过其使用文档较你全面，可以弥补这一缺点。

### 接收器

接收器除支持采集器输出的数据格式以外，还支持其他标准格式的数据输出。一般而言开源的数据采集器都会支持“缓存队列”的数据输出接口，在这种情况下，数据中心产品没有必要再提供单独的数据接收器。

对于其他（例如较旧的）日志输出方式（例如rsyslog），其不支持直接向缓存队列输出，所以需要提供独立的数据接收器。数据中心产品中使用开源软件Logstash作为（暂时的）数据接收器，但是Logstash占用的系统资源较多，具效率非常低（基于正则），在数据量较大的情况下无法满足性能要求。

使用独立的接收器，易于与解码器进行集成，简化系统结构。否则解码模块必需单独部署，不易于监控和管理。

### 缓存队列

当数据量较大时，需要使用“缓存队列”减轻解码及存储的压力。使用目前较流行的开源软件Kafka作为缓存队列，其性能表现相当优秀，且读写接口非常丰富。

### 解码器

解码器承担数据清洗的主要工作，包括格式化、数据标签、字段解释、过滤等功能。开源的解决方案有Storm、Spark等，但是对于自定义格式的数据解码，都需要二次开发。在数据量较小的情况下，开源的解决方案都会显得比较“重量级”，所以该模块需要根据需求进行研发，以应对“小客户”资源不足的应用场景。

无论使用开源解决文案或自行研发，解码器应包括但不限于如下功能：

* **格式化（标准化）**  
  对输入的数据进行标准JSON格式化，使其具备可读性（包括程序可读），并将具体的字段进行格式化，例如格式化时间戳、字符串转整型等功能。
* **数据标签**  
  对输入的数据增加额外的信息进行标记，例如根据用户ID增加用户名标识。
* **字段解释**  
  对枚举类的数值进行解释，例如将HTTP响应码200解释为“功能”，响应码大于400的解释为“失败”。
* **数据过滤**  
  支持输出过滤功能，提高数据的“纯净”度。

解码功能的配置支持可视化及脚本两种方式，以应对不同用户的需求。

# 数据存储

本章节描述数据中心产品中，数据存储功能的详细设计。

## 模块设计

数据存储包括实时存储、长期存储两个功能。数据中心产品使用ES（Elasticsearch）作为实时数据存储方案，该模块详细设计如图3-1所示：

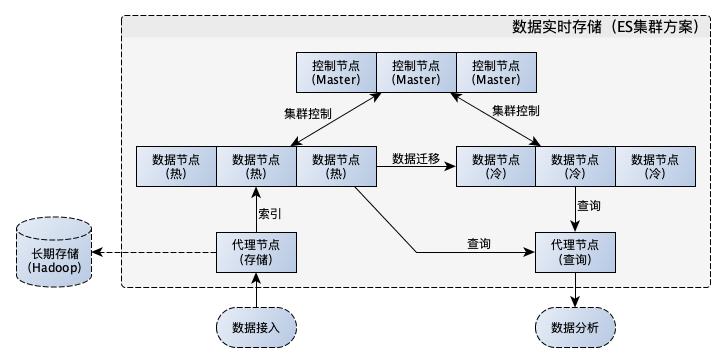


图 3‑1 实时存储模块（ES集群方案）

其中长期存储功能，为本系统（数据中心产品）中可选功能，因为长期存储需要用户的支持。由于数据中心产品一般情况下处理的数据量较大，所以选择业内已经成熟并广泛使用Hadoop作为解决方案。

## 模块说明

数据长期存储使用Hadoop作为解决方案，不在本文档描述范围内。而实时存储则使用ES集群，并没有模块的概念，本小节后续内容从功能方面着手进行详细描述。

### 控制节点

控制节点对应ES集群中的Master节点，其主要功能是管理其他节点，包括节点添加、服务发现、数据全局索引等功能。控制节点不承担数据存储与查询功能，因此无需其数据相对较少。但控制节点相当于集群的“大脑”，一旦宕机整个集群将无法使用。

### 数据节点

数据节点在ES集群中承担存储、查询等功能，对系统资源要求较高，包括内存、磁盘（容量及IO）。ES提供的强大的数据聚合功能，也是由数据节点直接执行，故而数据节点在集群中的角色较为重要。

### 输入/输出代理

输入/输出代理主要接收其他模块的索引及查询请求，并将请求发送给涉及的数据节点，在数据节点将数据返回之后，再将最最终的结果集进行排序。该类节点主要处理集群的I/O（Input/Output）请求，根据用户数据访问量来设定节点个数，一般情况下一个代理点即可满足大多数据的应用场景。

代理节点对应ES集群中的Client节点，可由Master节点“兼职”，但是在数据量较大时，一般设置独立的代理节点，以减轻控制节点的压力。

### 数据管理

数据管理，是指对ES集群中存储的数据进行管理，包括冷热分离、数据清理等功能，具体包括：

* **冷热分离**  
  将最新产生或者经常查询的数据，与“老旧”的数据或偶尔查询的数据分离开来，使用不同的数据节点存储，以提高系统资源的使用率和集群的响应时间。
* **分片及副本**  
  通过分片控制系统数据节点的负载均衡；通过副本来保证数据的安全性。
* **数据迁移**  
  定期将“热”节点数据转移到“冷”节点上，以提升热节点的响应时间。
* **数据删除**  
  定期删除“老旧”的数据（例如三个月前的数据），以提供更多的空间存储新数据。

除以上所述内容外，数据管理还包括索引管理、段合并等功能，详细请阅读ES用户使用手册。

# 数据分析

本章节描述数据中心产品中，数据分析功能的详细设计。

## 模块设计

数据分析包括可视化分析和自动化分析两个方面功能。可视化分析，要求数据中心产品为用户提供可视化的分析工具，以满足用户的自定义分析需求；自动化分析，要求数据中心产品提供规则引擎，自动进行重复性的分析，并生成分析结果。

该模块详细设计如图4-1所示：

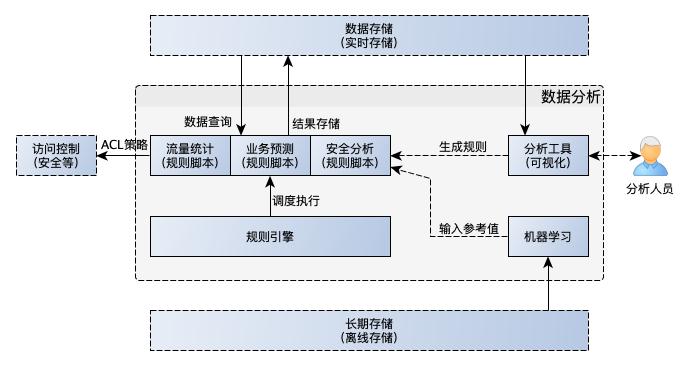


图 4‑1 数据分析模块设计

## 模块说明

本小节描述数据分析功能中各模块的详细设计，其中机器学习属于AI范畴，不在本文档描述范围之内。

### 规则脚本

数据分析基于“数据+规则”的方式进行设计，规则概念的提出相对久远，但是与数据结合（特别是大数据）以后，将发挥更大的威力。

数据中心产品通过脚本的方式实现规则，具备以下优势：

* **高度定制**  
  数据输入、检测策略、对比策略、时间模型、分析维度、结果输出等均由脚本控制，规则所有内容皆由用户自定义，满足各种用户对分析模型的需求。
* **复杂规则**  
  使用脚本进行“程控”，可制定出更复杂的检测规则。
* **高扩展性**  
  通过扩展脚本功能，在满足兼容的同时，可以对规则进行“无限”扩展。

### 规则引擎

规则引擎的实质就是规则脚本的解释器，与此同时，还提供了一定的调度策略。例如，可设置规则脚本在08:00到18:00执行；或者在11月11日暂停执行等调度策略。

### 分析工具

数据中心产品为用户提供可视化的数据分析工具，方便用户自行对数据分析。可视化的数据分析工具，跟数据展示模块结合（集成）在一起，以提供统一的用户入口。

数据分析工具提供最基本的两个功能：

1. **关联分析**  
   用户可以使用相同的过滤条件，分析不同的数据源、不同的数据维度、不同的数据指标。
2. **下钻分析**  
   支持用户至顶而下的分析方式，从异常的统计指标入手分析到产生异常的详细数据记录。

用户可通过分析工具设置固定的分析模型（指标、维度及步骤等），以简化其操作。

### 机器学习

数据中心通过对离线数据进行机器学习，找出数据之间的关联以及历史数据的指标参考值，并输出到实时分析模块作为参考。

# 系统管理

本文档描述数据中心产品中，系统管理功能（包括配置管理、监控等）的详细设计。

## 模块设计

系统管理是指对数据中心产品中所有模块的配置、管理、监控等，为系统运维人员提供集中式的管理和监控入口。其模块设计如图5-1所示：

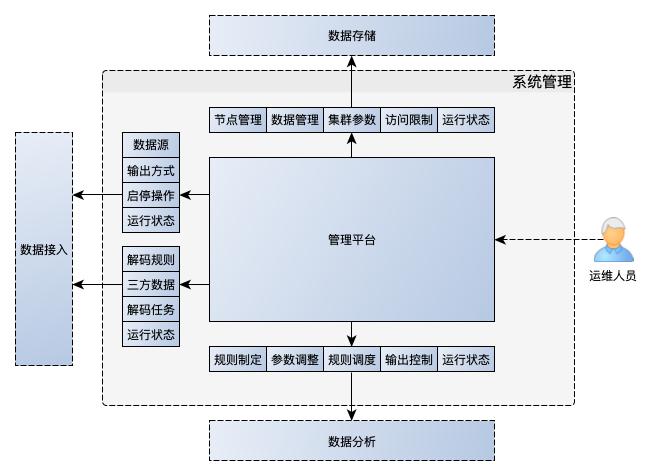


图 5‑1 系统管理

## 模块说明

系统管理功能的设计目标，是对数据中心产品所有环节进行管理和监控。其模块设计依赖于数据中心产品其他模块的设计，详细请参阅其他模块及独立的“系统管理设计文档”。

# 数据可视化

数据可视化模块，提供数据的展示功能，请参阅“数据可视化设计文档”。