ICS 35.240.01

# 中国仿真学会团体标准

T/CSFSIM 001—2024

# 工业应用软件安全云接入技术要求

Industrial application software secure cloud access technical requirements



2024-02-28 发布　　2024-03-13 实施

中　国　仿　真　学　会　　发布

# 目　次

# 前　言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由中国仿真学会提出并归口。

本文件起草单位：北京交通大学、东莞市康瑞电子有限公司、北京航空航天大学、中建一局集团华南建设有限公司、中科世安技术有限公司、广东海洋大学、中国铁路网络有限公司、北京中泓升环境科技有限公司、北京中科智上科技有限公司、青岛东坤蔚华科技有限公司、惟精环境科技有限公司、北京恒拓新天电力工程设计有限公司、河南亚盛电气有限责任公司、陕西路易德路桥技术有限公司。

本文件主要起草人：张振江，张阳，周孝恒，杨永丽，宋晓，丁鹏，李伟，李梦林，李昭，刘默涵，焦志伟，冼文杰，王九龙，寇广毅，王宇赫，马骁骅，曲鹏，杨玉山，赵绍豫，丁旭。

# 工业应用软件安全云接入技术要求

## 1 范围

本文件规定了工业应用软件安全云接入平台数据安全接入、传输、集成的技术要求。

本文件适用于工业制造企业相关的工业应用软件使用者，为使用安全云接入产品提供技术说明以及环境需求，也可用于指导相关安全防护技术的研制和开发。

## 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25067-2020 信息技术 安全技术 信息安全管理体系审核和认证机构要求

GB/T 40690-2021 信息技术 云计算 云际计算参考架构

GB/T 40693-2021 智能制造 工业云服务 数据管理通用要求

## 3 术语和定义

GB/T 40690-2021、GB/T 40693-2021、GB/T 25067-2020 界定的以及下列术语和定义适用于本文件。

3.1

**容器化 containerization**

将应用程序和所需的所有组件（例如库、框架和其他依赖项）打包在一起，让它们隔离在自己的“容器”中的过程。

3.2

**多协议适配 multi-protocol adaptation**

在不同通信协议之间建立连接，使不同设备或系统能够相互通信。在通信过程中对数据进行适当的协议转换和格式调整，以确保数据能够正确传输和解释。这种技术在跨越不同的领域和行业中广泛应用，包括物联网（IoT）、工业自动化、通信网络和云计算等领域，以兼容各种设备和系统的互操作性。

3.3

**云服务总线 cloud service bus**

一种云计算架构中的集成和通信模式，用于促进不同组件、应用程序和服务之间的通信和数据交换。它作为一种云中间件或消息传递服务提供，用于支持分布式系统中的松耦合通信。

3.4

**虚拟专用网络 virtual private network**

一种通过加密和隧道技术将工厂网络与云平台连接的方法，以确保数据传输的私密性和安全性。这种方法常用于保护敏感数据的传输，确保数据不被未经授权的访问者获取。

## 4 缩略语

下列缩略语适用于本文件。

AMQP：高级消息队列协议（Advanced Message Queuing Protocol）
CA：证书认证机构（Certification Authority）
CAS：中央认证服务（Central Authentication Service）
CoAP：受限应用协议（Constrained Application Protocol）
CSB：云服务总线（Cloud Service Bus）
HTTP：超文本传输协议（Hypertext Transfer Protocol）
HTTPS：超文本传输安全协议（Hypertext Transfer Protocol Secure）
JSON: JavaScript 对象表示方法（JavaScript Object Notation）
JWT：JSON Web 令牌（JSON Web Token）
LDAP：轻量目录访问协议（Lightweight Directory Access Protocol）
MAC：消息认证码（Message Authentication Code）
MQTT：消息队列遥测传输（Message Queuing Telemetry Transport）
OAuth2.0：开放授权协议的 2.0 版本（Open Authorization 2.0）
SSL：安全套接层（Secure Sockets Layer）
XML：可扩展标记语言（Extensible Markup Language）

## 5 工业应用软件安全云接入功能与技术要求

### 5.1 工业应用软件安全云接入功能架构及要求

#### 5.1.1 功能框架要求

工业应用软件安全云接入的功能框架如图 1 所示，包含了工业系统接入到功能框架，以及上游应用进行服务调用的过程。

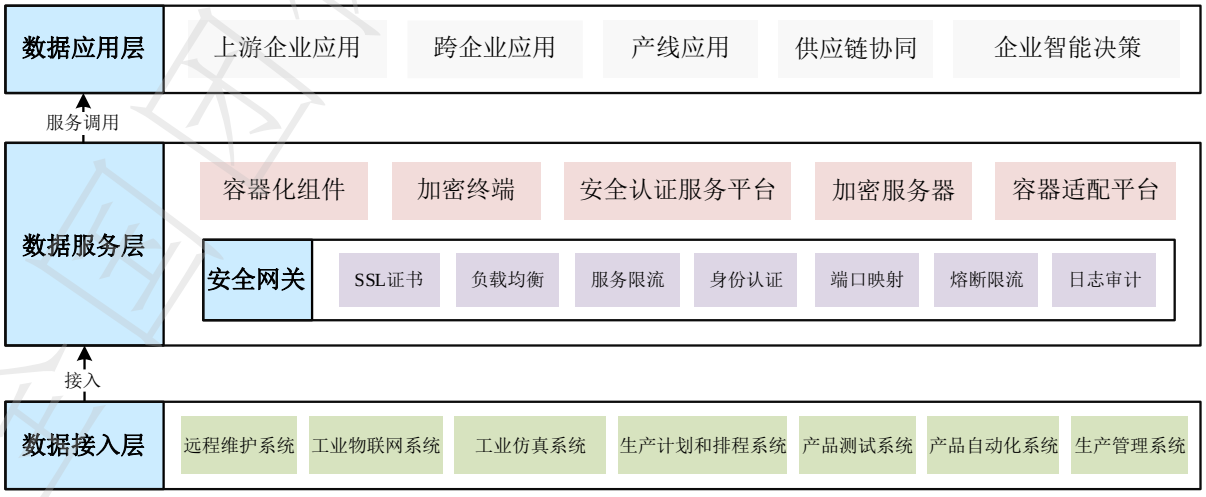


图 1 工业应用软件安全云接入功能框架

#### 5.1.2 容器化组件

容器化组件保障应用程序的可移植性和灵活性，使其能在多种设备环境中运行。要求如下：

a) 环境要求：适用于云、工业互联网、物联网设备等各种环境；

b) 技术要求：支持将组件打包为容器，以便有效地运行容器化应用程序；
c) 功能要求：容器内的软件或应用能够在任何环境和任何基础架构上一致地移动和运行，不受该环境或基础架构的操作系统影响。

#### 5.1.3 加密终端

加密终端用于保护数据传输、存储和处理的安全性。要求如下：
a) 环境要求：适用于需要数据加密传输的场景；
b) 技术要求：支持硬件快速实现多种加密算法，具有安全的密钥保护机制；
c) 功能要求：能够对用户进行身份认证，并使用加密算法对数据进行保护，确保敏感信息在传输和存储过程中不会被未经授权的人员访问。。

#### 5.1.4 安全认证服务平台

安全认证服务平台确保只有授权实体能访问系统或数据。要求如下：
a) 环境要求：支持运行安全认证服务所需的运行环境；
b) 技术要求：支持用户身份验证、访问控制和用户行为审计相关技术；
c) 功能要求：负责用户进入 CA 认证服务的网络信任域和工业专网应用服务系统前的接入和访问控制，具有用户身份认证代理的功能，能够和证书认证服务系统交互，完成用户身份认证，根据认证结果核对该用户的可信网络访问权限，完成网络接入的鉴权控制。

#### 5.1.5 加密服务器

加密服务器处理数据加密和解密操作，保障数据机密性。要求如下：
a) 环境要求：可部署于云端和本地环境中；
b) 技术要求：支持强大的加密算法和密钥管理机制，以确保数据的机密性、完整性和可用性；
c) 功能要求：能够运用多种加密算法对云上工业数据进行可靠的加解密运算，完成数据保护，同时满足数据安全方面的监管合规要求。

#### 5.1.6 容器适配平台

容器适配平台在不同设备和环境中部署和管理容器化应用程序。要求如下：
a) 环境要求：适应多种操作系统和硬件架构；
b) 技术要求：支持支持大规模容器的适配管理，并保持良好的性能和稳定性；
c) 功能要求：作为底层结构负责适配各种异构工业设备的数据接口，完成云平台的统一接入。

### 5.2 工业应用软件安全云接入技术架构及要求

#### 5.2.1 技术框架要求

工业应用软件安全云接入服务的技术框架如图 2 所示，包含了主要的技术要求：云服务多协议适配要求、工业软件的云服务网关要求。

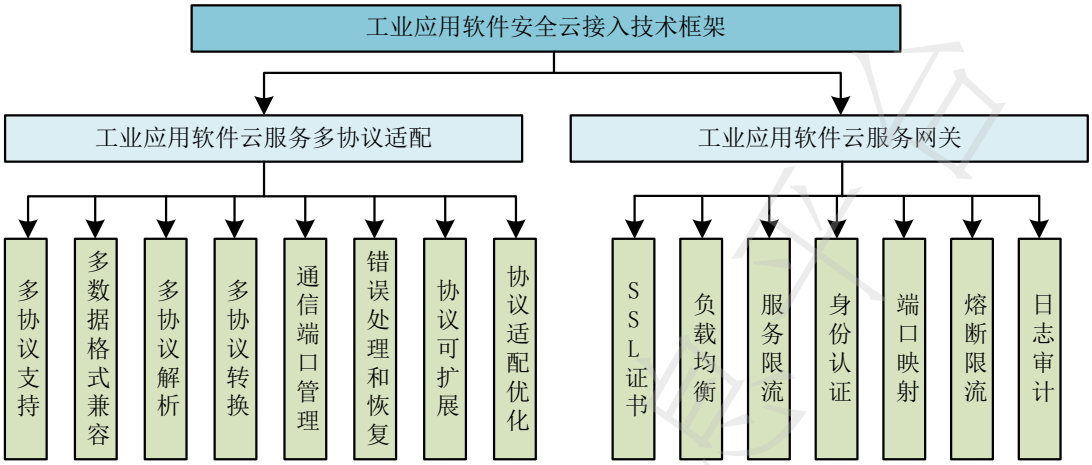


图 2 工业应用软件安全云接入技术框架

### 5.2.2 工业应用软件的云服务多协议适配要求

工业软件的云服务多协议适配要求是指确保工业软件能够与不同的通信协议进行适配和互操作的技术规范和要求。这些要求包括以下方面：

a) 协议支持：工业软件应具备支持多种通信协议的能力，包括但不限于 HTTP/HTTPS、MQTT、CoAP、AMQP 等，以适应不同设备和系统的通信需求；
b) 数据格式兼容性：确保软件能够处理和兼容不同协议中的数据格式，包括文本、二进制、JSON、XML 等；
c) 协议解析：能够解析和理解各种协议中的数据格式，以便对数据进行处理和分析；
d) 协议转换：软件能够进行协议转换，将一种通信协议的数据转换为另一种协议的数据，以确保不同设备之间可以无缝通信；
e) 通信端口管理：提供能够动态分配和管理通信端口的机制，以便不同协议的数据可以正确路由到相应的端口；
f) 错误处理和恢复：在协议适配过程中，能够处理错误和异常情况，采取适当的措施来确保通信的可靠性和稳定性；
g) 协议扩展性：支持添加新的通信协议或自定义协议，以应对未来的需求变化；
h) 协议适配优化：能够优化协议的适配过程，以确保低延迟、高吞吐量和高效能的通信。

### 5.2.3 工业应用软件的云服务网关要求

#### 5.2.3.1 SSL 证书

SSL 证书确保通信过程的安全性。SSL 证书技术要求如下：

a) 支持密码协商功能，能够在线协商通信两端共用的密钥交换算法、加密算法和 MAC 算法，并根据协商的密钥交换算法，完成通信的共享密钥协商；
b) 支持数据机密性保护功能，能够根据协商好的共享密钥和加密算法，加密需要传输的数据，确保数据的机密性；
c) 支持数据完整性保护功能，能够根据协商好的共享密钥和 MAC 算法，验证所传输数据的完整性。
d) 能够处理 HTTP 和 HTTPS 之间的协议转换，确保数据机密性和完整性保护功能的实现。

#### 5.2.3.2 负载均衡

负载均衡用于优化系统性能和资源分配。负载均衡技术要求如下：

a) 实施负载均衡策略，以平衡流量并分发请求给不同的微服务；
b) 选择适当的负载均衡算法，并确保负载均衡器的高可用性，负载均衡器需支持多种算法，如轮询、最少连接等。

#### 5.2.3.3 服务限流

服务限流可以防止服务过载和滥用。服务限流技术要求如下：

a) 在服务出现故障或性能下降时，自动停止对该服务的请求，以防止对其进一步施加压力；
b) 限制来自单个客户端或单位时间的请求次数，以防止滥用或恶意攻击；

#### 5.2.3.4 身份认证

身份认证保障系统访问的安全性。身份认证技术要求如下：

a) 支持多种身份认证方式：包括用户名密码、关键字、JWT 令牌、OAuth2.0、LDAP 协议、CAS 协议等；
b) 建立安全的身份验证流程，确保只有合法用户或设备能够访问系统。

#### 5.2.3.5 端口映射

端口映射增强不同系统通信协议间的兼容性。端口映射技术要求如下：

a) 支持多种通信协议的端口映射，以确保异构系统之间的互操作性；
b) 通过协议适配器或协议网关来进行协议的映射和转换。

#### 5.2.3.6 熔断限流

熔断限流防止系统过载和服务不稳定。熔断限流技术要求如下：

a) 实施熔断机制和请求限流策略，以应对异常请求和过度的流量负荷；
b) 支持基于阈值的限流和自动熔断不稳定的服务，以保护系统的稳定性。

#### 5.2.3.7 日志审计

建立全面的日志审计系统，记录各类访问请求的详细信息，包括身份验证、请求内容、响应结果等。审计内容包括系统中各类访问请求的详细信息，涵盖身份验证、请求内容和响应结果等。

## 6 工业应用软件安全云接入、传输、集成技术要求

### 6.1 云接入技术应用对象

不同的工业企业会使用各种应用软件接入云平台，具体使用的软件取决于其行业、需求和特定用例。表 1 中是本技术所适用但不限于的实际工业生产应用领域：

表 1 工业生产应用领域

| 序号 | 工业应用软件类型 | 应用场景与作用 |
|---|---|---|
| 1 | 远程维护系统 | 用于远程监控工业设备、机器人、生产线和生产过程，以进行实时故障检测、预防性维护和性能优化。 |
| 2 | 工业物联网平台 | 用于连接、监控和管理物理设备、传感器和工业设备，以实现数据采集、分析和控制。 |
| 3 | 生产计划和排程系统 | 用于计划和排程生产活动、库存管理和供应链协调，以确保生产计划的执行。 |
| 4 | 供应链管理系统 | 用于跟踪和管理供应链、订单处理、库存和交付，以提高供应链的可见性和效率。 |
| 5 | 工业安全管理系统 | 用于监控工业设备、入侵检测、视频监控和网络安全，以确保工厂和设施的安全性。 |
| 6 | 生产管理系统 | 用于整体管理和监控生产过程，从原材料采购到成品制造。实现生产过程的优化，提高生产效率，减少浪费，确保生产计划和目标的顺利实现。 |
| 7 | 产品测试类系统 | 用于在产品开发和制造过程中进行各种性能和安全性测试。保证产品符合质量标准和安全规范，提高产品的可靠性和市场竞争力。 |
| 8 | 产品自动化系统 | 用于自动化控制生产线和机器人，实现生产过程的自动化。提高生产效率和一致性，减少人为错误，降低劳动成本，增强生产灵活性。 |
| 9 | 工业仿真系统 | 用于将工业系统中的各个模块转化成数据整合到一个虚拟的系统中，在虚拟系统中模拟实现工业作业中的每一项工作和流程，并与之实现各种交互。 |

## 6.2 云接入数据传输要求

### 6.2.1 数据接入范围

云接入工业应用软件的数据接入主要包括但不限于以下几个方面：

a) 实时生产数据：包括来自工厂设备、传感器和监控系统的实时数据，如温度、湿度、压力、电流等；
b) 设备状态和健康数据：工业设备的状态信息，例如设备是否运行正常、是否需要维护、预测性维护的数据，以及设备的健康状况；

c) 质量数据：关于产品质量的数据，包括检测、测量和测试结果；
d) 供应链数据：与供应链相关的信息，如供应商交付状态、库存水平、订单状态等;
e) 能源消耗数据：关于工厂能源使用的数据，包括电力、水、气体等资源的消耗情况；
f) 操作日志和事件数据：关于工业过程中的事件和操作日志的数据，用于追溯、安全性和合规性监测；
g) 生产计划数据：包括生产计划的详细信息，如生产订单、计划产量、生产排程等；
h) 生产过程数据：涵盖生产线上的实时过程数据，例如生产速率、设备运行状态、工艺参数等；
i) 安全监控数据：与工厂安全性相关的数据，如监控视频、入侵检测、火警报警等；
j) 分析和报告数据：从工业应用软件中生成的报告、趋势分析、预测分析等数据。

### 6.2.2 数据接入方式

当使用云平台接入工业应用软件时，数据接入方式根据具体需求和架构进行选择，以确保数据的安全性、可靠性和高效性。数据接入方式包括但不限于以下几种：

a) 云服务提供商的 API：云服务提供商提供 API（应用程序编程接口）允许工业应用软件与云平台进行通信，这些 API 可用于将数据从工厂设备、传感器或其他系统传输到云中，也可以用于从云中检索数据；
b) 物联网（IoT）协议：工业设备和传感器使用物联网协议（如 MQTT、CoAP、AMQP 等）来将数据发送到云平台，这些协议完成实时数据传输，并支持设备之间的通信；
c) 消息队列：使用消息队列系统（如 Apache Kafka、RabbitMQ 等）将数据传输到云中，这种方式可用于完成异步数据传输和处理，以应对大量数据；
d) 批处理和文件传输：数据以批处理的方式从工业设备中收集，并通过文件传输协议（如 FTP、SFTP）将数据上传到云中，这种方式适用于周期性数据采集；

### 6.2.3 数据软件接口要求

数据软件接口要求确保云平台服务的高效、安全、灵活使用。接口如下：

a) 云计算服务接口：要求支持根据需求动态扩展或收缩计算资源，需要指定扩展规则和策略；
b) 云存储服务接口：要求平台能够通过云存储服务的方式实现文件的上传和下载，需要提供有效的身份验证和文件路径等参数，接口要求包括对象的创建、删除、更新等操作，需要提供对象的唯一标识符和相关元数据；
c) 网络服务接口：要求平台通过云平台的网络服务进行虚拟网络的创建、配置和管理，需要定义网络拓扑、子网等信息；
d) 数据库服务接口：要求平台通过云平台的数据库服务进行数据库的增删改查等操作，需要提供数据库名称、表名和操作类型等参数；
e) 身份与访问管理接口：要求平台通过云平台的身份与访问管理验证用户身份，涉及用户名、密码或访问令牌等验证方式，接口要求包括用户权限的设置和管理，需要指定用户、资源和权限等参数；
f) 日志与监控接口：要求平台能够获取云资源使用情况的日志信息，明确指定日志类型、时间范围等参数，要求平台能够获取资源的性能和使用数据，包括 CPU 利用率、内存使用等监控指标；
g) 消息队列和通知服务接口：要求平台通过云平台提供的消息队列服务实现异步消息传递，需要定义消息内容、队列名称等参数，接口要求包括事件触发的通知机制，需要指定触发事件和通知方式等参数。

### 6.2.4 数据接口协议统一要求

数据接口协议统一要求确保数据接口的一致性和高效性。要求如下：

a) 通信协议：选择统一通信协议，如 HTTP/HTTPS、MQTT、CoAP、AMQP 等，以确保不同系统之间的通信方式一致；

b) 通信方法：定义一致的通信方法，包括请求-响应、发布-订阅等，以满足不同场景的需求；
c) 身份验证和授权：实施一致的身份验证和授权机制，以确保只有授权的系统或用户能够访问数据和功能；
d) 消息格式：在通信协议中定义一致的消息格式，包括请求和响应的结构，以简化消息处理；
e) 错误处理：定义一致的错误代码和错误处理方法，以便远程系统能够识别和处理错误情况；
f) 性能和可伸缩性：发挥通信协议的性能和可伸缩性，以应对大量数据和高并发请求；
g) 版本管理：确保有一致的版本管理策略，以减少向后不兼容性；
h) 监控和日志：实施统一的监控和日志记录机制，以便跟踪通信和信息系统状态，帮助故障排除和性能优化。

#### 6.2.5 数据安全传输要求

##### 6.2.5.1 数据加密

数据加密保障数据在传输过程中的安全和机密性。要求如下：
a) 使用强加密算法（如 TLS/SSL）来保护数据在传输过程中的机密性；
b) 使用最新的安全协议和密码学标准，避免使用已知的弱加密算法和协议。

##### 6.2.5.2 身份验证

身份验证确保数据接口的安全访问。要求如下：
a) 实施双向身份验证机制，确保云平台和工业应用之间都能验证对方的身份。实现方式包括数字证书或身份令牌等；
b) 采用强密码策略，并实施多因素身份验证，以保护访问接口的凭证不被滥用。

##### 6.2.5.3 访问控制

访问控制管理和限制接口的访问权限。要求如下：
a) 确保只有经过授权的用户或系统能够访问接口。使用访问控制列表（ACL）或基于角色的访问控制来管理权限；
b) 实施适当的授权策略，以限制访问特定数据和功能。

##### 6.2.5.4 数据完整性

数据完整性确保数据在传输中的完整和未被篡改。要求如下：
a) 使用消息完整性校验，如哈希函数，以确保数据在传输过程中没有被篡改或损坏；
b) 确保只有授权的用户具有数据修改的权限，以防止未经授权的修改。

##### 6.2.5.5 日志和审计

日志和审计记录监控接口的通信。要求如下：
a) 记录接口通信的详细日志，包括请求、响应、时间戳和相关事件信息；
b) 定期审计日志以监测潜在的安全问题，并采取适当的措施来应对异常活动。

##### 6.2.5.6 防御性措施

防御性措施可以防止常见的网络安全威胁。要求如下：
a) 针对常见的安全威胁，如 SQL 注入、跨站脚本（XSS）等，实施防御性编程措施，以防止攻击；
b) 定期更新和维护所有依赖的库和框架，以修补已知的安全漏洞。

#### 6.2.5.7 数据隐私保护

数据隐私保护能够保护企业和个人隐私权利，防止敏感数据的滥用和泄露。要求如下：

a) 采用数据脱敏、数据最小化和数据掩码等技术，以减少敏感数据的传输和存储；
b) 遵守适用的数据隐私法规和标准，如《中华人民共和国数据安全法》、网络安全等级保护 2.0 制度。

#### 6.2.5.8 应急响应及处置预案

制定完善的应对工业安全事件和漏洞的应急响应及处置预案，以快速识别、应对和修复潜在的安全问题。

#### 6.2.5.9 定期安全审查

定期对接口和通信流程进行安全审查和渗透测试，以发现并纠正潜在的漏洞和风险。

### 6.3 云服务集成要求

#### 6.3.1 云服务总线技术要求

云服务总线（CSB）是一种云计算架构中的集成和通信模式，用于促进不同组件、应用程序和服务之间的通信和数据交换。云服务总线的技术要求应至少包括以下方面：

a) 通信中介：云服务总线作为通信中介，允许不同的应用程序、微服务、组件或系统之间通过消息传递进行异步通信；
b) 消息传递：云服务总线通过消息队列或主题（Topic）来传递消息；
c) 异步通信：云服务总线支持异步通信模式，发送者和接收者不需要同时在线或立即响应；
d) 负载均衡：云服务总线提供负载均衡机制，以确保消息被平均分配到可用的接收者；
e) 安全性和可靠性：云服务总线提供安全性功能，包括身份验证、授权、消息加密和访问控制；
f) 监控和管理：云服务总线提供监控和管理工具，以跟踪消息流量、性能指标和故障排除。

#### 6.3.2 基于云服务总线的服务集成要求

服务集成要求包括：

a) 服务可用性：确保系统中的服务在需要时可用，实施高可用性架构，包括负载均衡、故障转移和自动恢复机制，以减少服务中断的可能性；
b) 服务编排引擎：开发或使用强大的编排引擎，能够有效管理和调度各种服务的部署和执行，包括自动化决策和资源优化功能；
c) 编排可视化功能：提供用户友好的可视化界面，以便管理员和操作人员能够轻松创建、管理和监控服务编排流程，包括图形化工具和仪表板；
d) 服务接口：定义清晰的服务接口和 API 标准，以支持不同组件之间的通信和集成；
e) 服务节点响应时间：确保服务节点的响应时间在可接受范围内；
f) 服务节点权限控制：实施严格的权限控制机制，确保只有授权的实体能够访问和执行特定服务节点，包括身份验证、授权策略和访问控制列表；
g) 服务节点授权管理：建立有效的授权管理系统，包括用户/角色管理、权限分配和审计功能，以确保对服务节点的访问和操作进行跟踪和管理；
h) 节点间数据交互准确性：确保服务节点之间的数据传输和交互准确无误，要求实施数据验证、完整性检查和错误处理机制；
i) 服务编排功能可用性：保障编排功能的高可用性，以确保服务的连续编排和执行，包括故障恢复和备份机制；

j) 流程容错：实施容错机制，以处理意外情况和错误，确保服务编排流程的稳定性和可靠性；
k) 整体服务流程：定义整体的服务流程，包括流程步骤、依赖关系和触发条件，保证服务的有序执行；
l) 容器可用性：确保容器的高可用性，包括容器编排和容器运行时的管理，以防止单点故障和服务中断；
m) 服务跨平台性：确保服务可以跨不同平台和环境进行部署和执行。