

**云网运维服务能力白皮书**

**广东亿迅科技有限公司**

目录

[一、 能力介绍 3](#_Toc75355042)

[1.1 能力概述 3](#_Toc75355043)

[1.2 运营体系 3](#_Toc75355044)

[1.3 服务保障流程 4](#_Toc75355045)

[1.3.1 运营管理流程 4](#_Toc75355046)

[1.3.2 流程体系建设 7](#_Toc75355047)

[1.4 主要服务内容 14](#_Toc75355048)

[1.4.1 巡检服务 14](#_Toc75355049)

[1.4.2 监控服务 21](#_Toc75355050)

[1.4.3 基础设施维保服务 22](#_Toc75355051)

[1.4.4 应用系统运维服务 23](#_Toc75355052)

[1.4.5 平台层运维服务 24](#_Toc75355053)

[1.4.6 网络服务 25](#_Toc75355054)

[1.4.7 信息安全服务 26](#_Toc75355055)

[1.4.8 应急保障和重大事件保障服务 26](#_Toc75355056)

[二、 流程落地工具支撑 26](#_Toc75355057)

[2.1 ITSM工单管理系统 26](#_Toc75355058)

[2.1.1 接入管理 27](#_Toc75355059)

[2.1.2 服务请求管理 28](#_Toc75355060)

[2.1.3 事件管理 29](#_Toc75355061)

[2.1.4 问题管理 31](#_Toc75355062)

[2.1.5 知识管理 31](#_Toc75355063)

[2.1.6 日常运维管理 32](#_Toc75355064)

[2.1.7 系统管理 33](#_Toc75355065)

[2.2 ITMP监控系统 38](#_Toc75355066)

[2.2.1 监控管理 39](#_Toc75355067)

[2.2.2 监控采集 40](#_Toc75355068)

[2.2.3 监控分析 41](#_Toc75355069)

[2.2.4 监控告警 41](#_Toc75355070)

[2.2.5 监控汇报 41](#_Toc75355071)

[2.2.6 告警应用：对接工单系统 42](#_Toc75355072)

[2.3 CMDB系统 42](#_Toc75355073)

[2.3.1 生命周期管理 42](#_Toc75355074)

[2.3.2 网络设备与IP段管理 43](#_Toc75355075)

[2.3.3 资源利用率管理 43](#_Toc75355076)

[2.3.4 配置项管理 43](#_Toc75355077)

[2.3.5 数据字典管理 44](#_Toc75355078)

# 能力介绍

## 能力概述



结合自主研发的自动化运维工具，提供以现场驻守、远程及二线支撑多种方式相结合的形式给用户提供全面的云平台运营运维服务，主要服务内容包括巡检服务、监控服务、基础设施维保服务、应用系统运维服务、平台运维服务、网络服务和应急重保服务等，保障客户业务系统安全运行，为客户提供安全、可靠、放心的服务。

## 运维体系



## 服务保障流程

### 运营管理流程

运营体系整体由申告处理、故障维护、数据分析等三大类事务构成。

#### 申告处理

故障申告处理工作主要由管控团队中的运维管控组、服务台、7\*24监控组、工单处理组共同完成。主要工作包括：

1. 工单处理组对于所分派的ITSM工单进行预处理，当遇到无法由本组资源完成的工单、需要专业组协调完成时，则对工单进行转派；如发生到重要事件或疑似重要事件，则反馈到运营管控团队的运维管控组，由运维管控组对事件进行跟进和处理。
2. 服务台和7\*24监控组如发现重要事件或疑似重要事件，同样反馈到融合运营团队的IT运维管控组，由运维管控组对事件进行跟进和处理。
3. 运维管控组对于2中所接收到的所有故障进行预判及技术支持，并做如下处理：
* 普通故障转运营管控团队中的技术前置协调组进行处理；
* 复杂故障立即组织技术前置协调组进行故障重现与确认，对于经过确认的故障立即由技术前置协调组根据“先抢通后抢修”的原则进行处理；
* 对于重大运营故障，在技术前置协调组处理的同时，运维管控组还须跟进故障处理进度，并及时运营管控中心通传通报。

#### 故障维护

故障维护由运营管控团队中的技术前置协调组协调数据库维护组、基础设施维护组、应用维护组、业务维护组等5个专业维护处理小组共同完成。主要工作包括：

1. 技术前置协调组接收故障的渠道包括：A、ITSM系统分派的工单；B、客户通过Q群、电话等其它渠道申告的紧急故障；
2. 技术前置协调组收到1中的客户申告后，应先进行前置干预处理，并根据故障紧急程度与严重程度采取相应的措施，“先抢通后抢修”，保证在故障发生十分钟内先期恢复生产；
3. 技术前置协调组在故障维护过程中，应注意识别重要事件及留意故障处理效果，一旦发现重要事件及故障遗留问题，应及时报事件与故障管控组进行后期持续跟进，推进此类故障的处理与解决；
4. 对于重大运营事故，技术前置协调组应在故障解决后组织资源对故障进行分析，编写《重大故障维护报告》，提交运营管理中心；
5. 技术前置协调组应定期组织各专业处理小组总结经典案例并编写相应的维护指南，交数据集成统计分析组进行知识库更新。

#### 数据收集分析与系统优化

数据收集分析与系统优化工作由融合管控团队中的数据集成统计分析组全权负责，主要工作包括：

1. 根据运维管理平台服务质量考核指标及系统性能预测的相关要求，定义数据统计指标、统计维度、统计方法与频度，定期进行数据收集与统计；
2. 定期发布运维管理平台服务周报，通报运维服务的运行情况、运维服务质量考核结果、重大事件/关键事件/遗留问题跟踪处理情况等；
3. 对系统性能进行前瞻性预测，根据系统运行的特定需要提出系统优化建议，提交技术前置协调组落实；
4. 定期收集专业处理团队编写的案例分析及维护指南，更新维护共享知识库。

附：运营管控流程图



图：运营管控流程

### 流程体系建设

#### 故障响应流程及规范

为保证故障发生时，能够有效的恢复业务，降低损失，系统故障应急处理遵循**“先抢通，后抢修”**的总原则，在较短时间内尽可能恢复业务，减少业务受影响的范围，缩短业务受阻的历时，应急处置须遵循四个原则：

1. **先抢通，后抢修原则**，即故障发生时，应急处置以最快恢复生产为目的，优先抢通系统运行，然后再分析问题，彻底排除故障。
2. **先核心，后周边原则**，分为两种情况：一种是，故障发生时，优先恢复核心系统的生产运行，后恢复周边系统的生产运行；第二种是，当故障导致资源出现瓶颈时，优先保证核心服务、核心系统的恢复和正常运行，在特殊情况下，可以停止非核心系统和业务，待故障修复后，再启动非核心服务或非核心系统。
3. **信息统一管控原则**，即故障发生后，对外信息的通传通报统一管理，统一发布，遵循应急管理规范的规定发布信息，无关人员不得发布相关信息。
4. **同架构、同设备关联巡检原则**，当应急处置稳定后，需要对同架构系统、同型号关联设备做巡检，以防故障衍生。

##### 故障响应

将根据申告的故障级别，采取必要的服务措施，尽快解决故障，恢复系统正常运行。可通过电话指导、远程登陆或现场服务等方式进行故障恢复，并保证满足约定的服务等级中相应故障级别的处理时限。

##### 故障级别定义

根据故障的严重程度和影响程度的不同，故障级别由高到低分为一级、二级、三级故障。

| **优先级** | **安全等级** | **影响等级** | **说明** |
| --- | --- | --- | --- |
| 一级故障 | 严重 | 非常高 | 紧急服务是指系统无法工作或受到严重影响。对业务有严重影响，用户不能执行日常工作，或者有严重的，负面的业务/财务影响。用户也不能通过其他方式执行日常工作。 |
| 二级故障 | 主要 | 高 | 指非紧急的服务，系统无法工作或受到影响。对业务有一定影响。用户在执行日常操作时有困难且在问题解决之前能够进行其他工作。 |
| 三级故障 | 一般 | 低 | 指非紧急的服务，系统无法工作或受到影响。对业务没有直接影响。问题给用方的员工带来了不便，用户可以通过其他方式执行日常工作。 |

##### 响应要求

|  |  |  |
| --- | --- | --- |
| **故障等级** | **响应要求** | **响应措施** |
| **工作时间** | **非工作时间** | **工作时间** | **非工作时间** |
| 一级故障 | 5分钟 | 10分钟 | 属地工程师现场处理，派遣专家到现场 | 远程技术支持，30分钟内派遣专家到现场 |
| 二级故障 | 10分钟 | 15分钟 | 属地工程师现场处理，派遣专家到现场 | 远程技术支持，45分钟内派遣专家到现场 |
| 三级故障 | 15分钟 | 30分钟 | 属地工程师处理 | 远程技术支持 |

##### 恢复要求

|  |  |
| --- | --- |
| **故障等级** | **恢复要求** |
| **工作时间** | **非工作时间** |
| 一级故障 | 15分钟 | 30分钟 |
| 二级故障 | 30分钟 | 1小时 |
| 三级故障 | 2小时 |

备注：数据恢复除外，数据恢复取决于坏件到货时间和恢复设备自身恢复时间。

##### 故障上报机制

如在规定时间内未能按照规定提供相应的服务，将根据故障处理情况向上级领导和用户领导汇报，具体汇报的对象和时限可根据下表：

| **未恢复业务所用的时间** | **一级故障** | **二级故障** | **三级故障** |
| --- | --- | --- | --- |
| **工作时间** | **非工作时间** | **工作时间** | **非工作时间** | **工作时间** | **非工作时间** |
| 15分钟 | 运营管控中心 |  | 运营管控中心 |  |  |  |
| 30分钟 | 运营管控领导小组 | 运营管控中心 | 运营管控领导小组 | 运营管控中心 |  |  |
| 1小时 | 公司高管 | 项目总负责人/客户IT管理层 | 公司高管 | 运营管控领导小组 | 运营管控中心 |  |

##### 故障恢复和故障解决

接到故障后，支撑人员直接到故障定位故障，属于日常支撑服务范围内，直接排查故障。否则派单到专业技术支撑团队运维管控组，由运维管控转派给专人负责解决。

对于影响业务的一级故障，在进行故障处理时，将优先考虑业务恢复，然后再彻底解决故障。

主要服务内容包括：

* 根据故障诊断结果及时进行故障排除，以保证尽快恢复系统的正常使用状态；
* 对于维护清单以外的非本项目系统产品故障造成的问题，工程师将给出合理的建议。
* 对未明确原因的问题，将协助用户进行排查。

##### 故障处理流程

###### 目标和职责

**目标：**接受用户报障，生成服务单，分派给指定的服务工程师对服务范围内的报障进行故障处理，使系统恢复正常运行。

**职责矩阵：**

|  |  |  |
| --- | --- | --- |
| 人员职责 | 用户方 | 支撑团队 |
| 主管部门 | 用户 | 服务台 | 服务工程师 | 服务经理 |
| 监督管理 | 负责 |  |  |  |  |
| 报障 |  | 负责 |  |  |  |
| 接障 |  |  | 负责 |  |  |
| 生成服务单 |  |  | 负责 |  |  |
| 处理故障 |  |  | 协调供应商 | 负责 |  |
| 故障分析报告 |  | 审核 | 负责 | 负责 | 负责 |
| 服务单归档 |  |  | 负责 |  |  |
| 新增知识库 |  |  |  |  | 负责 |

###### 工作程序

1. **故障告警及预处理:**
	1. 监控组和服务台在发现故障后，立刻进行定位，如属于应用故障，需在5分钟内发出告警通知。
	2. 对于业务中断的故障，后续每隔15分钟，通过短信通报处理情况。
	3. 服务台收到用户报障信息后，记录用户所提供的故障现象，填写《服务单》，属于紧急/非常重要的立刻转应急处理流程处理。
	4. 对于一般情况下的报障，服务台首先查询知识库，判断能否在电话中处理（简单的故障，用户可操作的情况下），如可以在电话中处理，将处理方法反馈用户，直接由服务台完成服务单，将服务单在服务台归档，结束服务。
	5. 如不能通过电话解决，服务台将按照故障类别将服务单分派给指定的服务工程师，服务工程师按故障处理流程解决故障，恢复服务运行。
2. **故障处理：**服务工程师收到服务台分派的服务单后，判断故障是否平台故障。如是，则协调应用系统技术处理。如否，则转由专业技术支持组处理，并做好以下措施：
	1. 维护组内部故障升级要求：无法评估解决的或者故障影响业务的时间超过10分钟。
	2. 对于业务中断的故障，每隔15分钟将处理进展反馈给监控组。
3. **完单：**故障处理完成后服务工程师提交故障分析报告，交用户确认后与相关文档一起返回服务台，服务台在收到服务工程师返回的处理结果后，将服务单及相关文档归档，结束服务。服务经理审核服务单后将有用的知识提取并生成知识点，加入知识库以便发生同类故障时参考。
	1. 故障分析报告，在故障修复后24小时内提交（可逐步完善）。
	2. 故障及处理、整改情况需要在下一周维护例会上总结，并且在维护月报中汇总。
4. **产出文档：**故障分析报告



## 主要服务内容

服务内容主要包括：运营服务巡检服务、监控服务、故障修复、数据备份与恢复、硬件运维服务等。第三方软件运维服务、基础设施保障服务、漏洞管理服务、网络运维服务、备品备件管理、自动化运维服务、应急保障服务。

### 巡检服务

运维组人员每日、每周、每月、每季度会定期进行系统及设备的检查并出具平台巡检报告，对当前平台的状况定期进行总结分析，了解当前平台状况，以及存在的问题和改进方法。

 包括机房巡检、设备巡检、系统平台巡检等。

* **目标和适用范围**

目标：通过对设备定期检测、维护和保养，保障设备运行稳定，通过保养延长设备生命周期，降低故障率。

适用范围：适用于设备的保养工作。

职责：

|  |  |  |
| --- | --- | --- |
| **人员****职责** | **用户方** | **维护方** |
| 主管部门 | 用户借口人 | 服务台 | 普查人员 |
| 监督管理 | 负责 |  |  |  |
| 巡检准备 | 确认巡检计划下发巡检通知 | 确认巡检时间配合巡检准备 |  | 编制巡检计划人员分组培训 |
| 现场巡检 |  | 配合确认结果 |  | 负责 |
| 巡检报告 | 审批确认 |  |  | 负责 |
| 归档 |  |  | 负责 |  |

* **工作程序**
* **巡检时间和巡检内容**

设备定期巡检，内容包括设备检测、设备除尘清洁与保养。

* **巡检准备：**
1. 维护方编写《巡检工作计划》，提交给用户审核后，由用户方主管部门下发给各用户接口人。
2. 用户接口人在收到普查计划后应确认上门巡检时间，向维护方提供巡检所需的资料，并做好巡检准备。
3. 维护方将巡检人员按巡检计划进行人员分组，并组织培训，规范巡检人员工作。
* **现场巡检：**
1. 巡检人员按照巡检计划安排用户接口人所在地开展现场巡检工作，检查设备状况，对设备进行清洁与保养。用户应安排专人现场陪同，协助巡检工作。
2. 巡检人员填写《巡检记录表》，记录巡检过程和结果，用户对巡检结果进行现场确认。
* **巡检报告：**
1. 巡检人员将收集的巡检记录表汇总分析后，形成《巡检报告》，根据巡检结果向用户提出存在的问题以及优化建议。
2. 用户方主管部门确认巡检报告。
3. 巡检记录表、巡检报告交服务台归档。
* **产出文档：**
1. 巡检工作计划
2. 巡检记录表
3. 巡检报告

#### 巡检流程



#### 日维护巡检内容表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **维护作业项目** | **周期** | **频次** | **交付物** |
| 1 | 7\*24小时远程监控，包括虚拟机资源、网络资源、云主机、存储资源、安全事件； 检查网络、主机、存储设备、虚拟化服务器和安全设备的运行情况；应用包括WEB、FTP、邮件、中间件、数据库等服务状态监控； | 日 | 提供需要检查的详细硬件设备清单，对新增的应用专门标注，每月1次 | 月维护作业实施记录表 |
| 2 | 检查应用系统的进程状态，清理异常进程 | 日 | 每日一次--提供需要检查的详细软硬件设备清单 | 附件：《项目日报表》-主机利用率 |
| 3 | 检查应用系统进程对CPU的占用情况 | 日 | 每日一次--提供需要检查的详细软硬件设备清单 | 附件：《项目日报表》-主机利用率 |
| 4 | 检查应用系统进程对内存的占用情况 | 日 | 每日一次--提供需要检查的详细软硬件设备清单 | 附件：《项目日报表》-主机利用率 |
| 5 | 查看系统的各种运行日志和错误日志 | 日 | 每日一次--提供需要检查的详细软硬件设备清单 | 附件：《项目日报表》-系统的运行日志和错误日志 |
| 6 | 检查应用系统数据对文件系统空间的占用情况 | 日 | 每日一次--提供需要检查的详细软硬件设备清单 | 附件：《项目日报表》-业务虚机明细 |
| 7 | 检查应用系统数据对数据库资源的占用情况 | 日 | 每日一次--提供需要检查的详细软硬件设备清单 | 数据库日常记录 |
| 8 | 重要数据表的备份 | 日 | 每日一次--提供需要检查的详细软硬件设备清单，虚机镜像备份也要检查，备份的具体内容。需增加重要数据的异地备份 | 附件：《项目日报表》-备份情况 |
| 9 | 对每日检查的数据用报表的形式，发送给相关的负责人 | 日 | 需要纸质记录材料，同时以报表形式发给相关负责人，每班一次。 | 附件：《项目日报表》 |

#### 周维护巡检内容表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **维护作业项目** | **周期** | **频次** | **交付物** |
| 1 | 检查应用系统的进程状态，进行汇总 | 周 | 每周一次 | 维护周报 |
| 2 | 检查应用系统进程对CPU的占用情况，进行汇总 | 周 | 每周一次 | 维护周报 |
| 3 | 检查应用系统进程对内存的占用情况，进行汇总 | 周 | 每周一次 | 维护周报 |
| 4 | 查看系统的各种运行日志和错误日志，进行汇总 | 周 | 每周一次 | 维护周报 |
| 5 | 检查应用系统数据对文件系统空间的占用情况，进行汇总 | 周 | 每周一次 | 维护周报 |
| 6 | 检查应用系统数据对数据库资源的占用情况，进行汇总 | 周 | 每周一次 | 维护周报 |
| 7 | 数广云平台重要数据的备份，并进行汇总 | 周 | 每周一次 | 维护周报备份文档 |
| 8 | 对每周检查的数据用报表的形式，汇总后发送给相关的负责人  | 周 | 每周一次 | 维护周报 |
| 9 | 增加网站安全监测内容 | 周 | 每周一次 | 维护周报 |
| 10 | 增加对安全设备、网络设备日志的检查 | 周 | 每周一次 | 维护周报 |
| 11 | 网站安全监测：根据站点管理者的监管要求，通过对目标站点进行不间断的页面爬取、分析、匹配，为客户的互联网网站提供远程安全监测、安全检查、实时告警，是构建完善的网站安全体系的最好补充。 | 周 | 每周一次 | 维护周报 |

#### 月维护巡检内容表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **维护作业项目** | **周期** | **频次** | **交付物** |
| 1 | 应用系统软件、运行日志、配置参数备份 | 月 | 每月一次 | 维护月报 |
| 2 | 运行日志清理、历史数据清理、垃圾数据清理等 | 月 | 每月一次 | 维护月报 |
| 3 | 对每月检查的数据用报表的形式，汇总后发送给相关的负责人 | 月 | 每月一次 | 维护月报 |
| 4 | 核心路由器、交换机设备cpu、内存利用率、板卡状态检查、软件升级管理；接口流量，特别是主干出口流量（平均值、峰值） | 月 | 每月一次 | 维护月报 |
| 5 | 数据库设备维护服务，包括检查数据库表空间状态、检查数据库表锁lock、sga内存使用状态、数据备份和安全评估等。 | 月 | 每月一次 | 维护月报 |
| 6 | 对服务器的性能进行全面检测，特别是对服务器处理大批量数据的情况下的CPU的占用率，内存的占用率等进行查看，以确保服务器的性能。 | 月 | 每月一次 | 维护月报 |
| 7 | 存储设备性能检测、空间分配与管理、日志查看和错误分析； | 月 | 每月一次 | 维护月报 |
| 8 | 系统数据及软件应用数据系统备份、检查；设备巡检报告收集和归档。 | 月 | 每月一次 | 维护月报巡检报告 |
| 9 | 设备硬件深度健康检查服务：现场对保修设备进行全面的健康检查，及时发现故障（或问题）的隐患，并协助排除系统故障或调整系统性能，同时做好设备的保养工作等。 | 月 | 每月一次 | 维护月报巡检报告 |
| 10 | 操作系统主动巡检服务：现场对操作系统进行全面的检查，及时发现故障（或问题）的隐患，并排除操作系统故障或调整操作系统性能等。 | 月 | 每月一次 | 维护月报巡检报告 |
| 11 | 数据库主动巡检服务:对数据库进行全面的检查，及时发现故障（或问题）的隐患，并排除数据库故障或调整数据库性能等。 | 月 | 每月一次 | 维护月报巡检报告 |
| 12 | 数据库主动巡检服务：对数据库进行全面的检查，及时发现故障（或问题）的隐患，并排除数据库故障或调整数据库性能等。 | 月 | 每月一次 | 维护月报巡检报告 |
| 13 | 虚拟化软件主动巡检服务：到现场对虚拟化软件进行全面的检查，及时发现故障（或问题）的隐患，并排除虚拟化软件故障或调整虚拟化软件性能等。 | 月 | 每月一次 | 维护月报巡检报告 |
| 14 | 同步不走实时接口的组织机构，工单状态，工单类型等维表数据 | 月 | 每月一次 | 维护月报 |
| 15 | 检查爬虫服务器、定时调度任务运行情况，确保爬虫服务器正常运行。 | 月 | 每月一次 | 维护月报 |
| 16 | 增加系统漏洞扫描（绿盟） | 月 | 每月一次 | 维护月报 |

#### 季度维护巡检内容表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **维护作业项目** | **周期** | **频次** | **交付物** |
| 1 | 定期审阅用户帐号、口令、权限 | 季度 | 每季一次 | 维护季报、季度维护作业实施记录表 |
| 2 | 虚拟化环境，设备CPU利用率情况检查，设备memory利用状况检查。 | 季度 | 每季一次 | 维护季报、季度维护作业实施记录表 |
| 3 | 虚拟化设备系统模块运行状况检查，设备电源及风扇检查。 | 季度 | 每季一次 | 维护季报、季度维护作业实施记录表 |
| 4 | 虚拟化设备系统LOG日志检查，设备冗余协议检查。 | 季度 | 每季一次 | 维护季报、季度维护作业实施记录表 |
| 5 | 虚拟化VLAN状态检查，EtherChannel检查，Trunk检查 | 季度 | 每季一次 | 维护季报、季度维护作业实施记录表 |
| 6 | 虚拟化路由状况检查，生成树STP检查，接口状态检查。 | 季度 | 每季一次 | 维护季报、季度维护作业实施记录表 |
| 7 | 线路巡检：对运维相关线路进行检测，将故障率将至最低，查看有无异常现象，并做好相应检查记录。 | 季度 | 每季一次 | 维护季报、季度维护作业实施记录表 |
| 8 | 安全测试：根据客户信息系统的现状制定安全测试指标和测试方案，为WEB应用、二进制程序以及移动APP提供全面的安全性测试服务，验证安全防护体系的完整性和有效性。 | 季度 | 每季一次 | 维护季报、季度维护作业实施记录表 |
| 9 | 漏洞扫描：通过远程安全检测的方式，批量发现工控设备、工控软件以及支撑他们运行的服务器、数据库、网络设备的安全风险。 | 季度 | 每季一次 | 维护季报、季度维护作业实施记录表 |
| 10 | Web应用漏洞扫描：可自动获取网站包含的相关信息，并全面模拟网站访问的各种行为，比如按钮点击、鼠标移动、表单复杂填充等，通过内建的"安全模型"检测Web应用系统潜在的各种漏洞，同时为用户构建从急到缓的修补流程，满足安全检查工作中所需要的高效性和准确性。 | 季度 | 每季一次 | 维护季报、季度维护作业实施记录表 |

### 监控服务

负责实施7X24小时实时监控工作，监控系统主旨建立统一的监控管理，监控采集，监控分析，监控告警，监控汇报的监控系统对监控设备进行不间断的实时监控，主要目的在于发现故障的第一时间及时通报相关人员，以此减轻甚至减免故障导致的不良影响。系统提供各种维度的管理功能，使运维体系的监控数据易管理，易维护，易扩展；系统提供多元的监控类型支持，多样的采集手段，使运维体系的监控范围更广；系统提供统一的告警处理，使运维体系中故障处理更加集中，更加高效，更加精准。除了及时发现故障，通报故障，处理故障，监控系统所产生的日常监控数据的汇总，亦可对整个运维体系的调整，扩展提供实质的数据参考作用。



### 基础设施维保服务

包括网络设备、主机设备、存储设备等第三方硬件设备，以及操作系统、备份系统等第三方软件系统的维保服务，有日常维护响应处理、高级技术支持服务等不同的服务项。定期到现场对保修设备和第三方软件进行全面的检查，及时发现故障（或问题）的隐患，并排除系统故障或调整系统性能，必要时更换故障部件，同时做好设备的保养工作等按约定周期定期对硬件设备和第三方软件运行状态进行检查和分析，完成检查和故障处理报告，确保设备运行正常，及时发现隐患并改进，保证业务连续性；及时解决硬件故障、为客户使用过程提供支持，保证系统稳定运行；提出改进建议，优化性能，提升设备运行稳定性及效率。

全面支撑各品牌硬件、操作系统，除承接硬件维保外，还可以提供保外设备支撑、盘活旧设备资源、增值运维、性能调优等服务

* **机房运维：**包括机房巡检、驻场维护、资产管理等
* 负责机房基础设施（动力、暖通、消防、弱电等系统）日常保养及维护支撑
* 负责7X24小时机房驻场维护、巡检、工程随工
* 负责重要事件的响应、跟进及实施专项保障工作
* **硬件设备：鲲鹏、飞腾、龙芯等芯片的PC终端及服务器、同有存储、国产网络设备等**硬件设备的的维保、故障处理和性能调优等
* 日常维护响应处理：硬件维保服务、故障处理
* 高级技术支持服务：技术支持服务、深度健康检查服务及调优
* **操作系统：麒麟、统信（深度）、中兴新支点、普华软件等**操作系统故障处理、性能调优与重保支撑等
* 日常维护需求响应与处理：日常维护需求响应与处理、故障修复服务、主动巡检服务
* 高级技术支持服务：重大事件现场顾问支持/保障服务（含应急预演服务）、参数配置优化服务



### 应用系统运维服务

包括对客户的技术人员提供技术支撑，以及升版支撑和运营数据统计与分析等。为系统的运维人员提供咨询、培训、知识库等，确保业务系统的正常生产运营；通过对运系统平台的营分析支撑和性能、应用优化分析与建议，提升系统的高效运营。面向应用软件，提供软件的升级服务，在软件故障发生时，需要通过升级解决故障保证软件的正常运行，根据系统的架构情况，开发相应的自动化升级脚本，并调优脚本的执行效率。

* **日常维护服务**
* **应用部署：**提供应用软件的部署方案设计、安装、配置、调测服务
* **应用日常维护：**应用启、停服务；程序运行监控、日常程序运行故障处理
* **高级技术支持服务**
* **应用软件升级服务：**常规升版服务（版本管控、升级实施服务、升版工具开发）、灰度升版服务（灰度升版项目建设、灰度升版）
* **应用迁移服务：**应用布署的主机扩展、域扩展、应用迁移（包括方案－评审－迁移实施－验证）
* **应急切换服务：**出现数据库或主机故障时，应用的快速应急切换处理（包括应急方案制定与评审、应急预演和应急切换实施）



### 平台层运维服务

数据库、中间件等平台层系统运维，提供数据库和中间的日常维护服务、高级技术支撑服务和新能优化服务等，包括日常维护需求响应与处理、故障修复服务、主动巡检服务、补丁与升级服务、性能分析和优化和重大事件现场顾问支持/保障服务（含应急预演服务）等，确保平台运行正常，及时发现隐患并改进，保证业务连续性，提出改进建议，预防潜在故障，优化性能，提升系统运行稳定性及效率。

* **中间件：金蝶、东方通、中创、宝兰德等国产中间件，以及weblogic、tomcat等非国产数据库**
* **日常维护服务：**中间件安装服务、故障修复服务、巡检服务
* **高级技术支持服务：**补丁与升级服务、调优服务、重保顾问支持/保障服务
* **数据库：人大金仓、达梦、南大通用、神舟通用等国产数据库，以及oracle、mysql等非国产数据库**
* **日常维护服务：**日常维护需求响应与处理、故障修复服务、主动巡检服务
* **高级技术支撑服务：**补丁与升级服务、迁移及数据清理服务、重保顾问支持/保障服务
* **性能优化服务：**优化方案制定、实施及验证



### 网络服务

* **网络规划设计：**依据相关设计的要求及标准，进行深化设计，编制完善的网络规划设计方案
* **网络集成实施：**按设计方案编制集成实施方案，并进行集成实施
* **故障处理：**主动监控网络设备、网络线路各项指标和运行状态，及时处理网络故障，保障网络稳定
* **网络安全：**对网络进行安全风险评估，确定系统漏洞与安全风险并进行网络安全防护、加固及整改
* **网络优化：**针对现有网络现状并结合现网流量模型和应用情况，评估、分析当前网络存在主要问题并给出详细优化方案，针对关键问题需要给出测试方案和实施方案

### 信息安全服务

**1）安全检测**

安全检测主要包含安全测试、渗透测试、网络入侵检测、工控漏洞扫描、Web应用漏洞扫描、网站安全监测。

**2）安全监控**

安全管理与监控服务：帮助用户实现全天24小时监控、24小时事件响应和专业安全管理，包括安全监控服务和安全管理服务

**3）安全防护**

安全防护主要包含网络入侵防护、WEB应用防护、数据泄露防护、抗拒绝服务。

**4）安全运维**

安全运维主要包含安全加固、日常运维、应急响应、信息安全演练。

### 应急保障和重大事件保障服务

充分利用各方资源，确保在发生重大事故时，能尽快解决故障，恢复系统可用性，将影响降至最低程度，提高应急保障响应速度和反应能力，确定应急恢复计划的范围与目标，设计提供应急恢复方案，以保证业务的持续性和可用性。

重大事件保障期包括汛期、重大节假日、国家军事、政治活动等期间需保障全系统维保清单范围内所有设备的正常运行并提供相应的重保方案、应急预案、事前深度巡检报告。

# 流程落地工具支撑

##  ITSM工单管理系统

工单管理系统总体目标是以支撑企业战略转型为目标，以提升客户体验为中心。借助支撑工具，通过流程化的管理方法实现管控体系与技术体系的有机结合，以可衡量的方式高效率完成企业IT支撑体系相关的规划与设计、建设与交付、运营维护及持续提升。

工单管理系统目标是建立IT服务管理的基本框架，改善IT客户的服务体验，提高IT运维的效率。具体目标包括：

* 建立统一的客户服务界面，提高客户对服务的感知。
* 固化运维类相关流程，包括：服务请求管理、接入管理、事件管理、问题管理、知识管理、日常运维管理等管理，提高IT服务管理的规范性。
* 工单系统提供灵活的可视化流程配置功能，能够满足各种复杂流程上线、快速变更的业务需要，后期补充固化日常需求管理、变更管理、发布管理、测试管理、配置管理等流程，实现完整的IT支撑体系。

### 接入管理

接入管理是对IT用户访问企业信息化部管辖范围内的IT基础设施或业务系统的数据库和操作系统的访问权限进行申请、审批、分配、回收的管理流程，包括帐号、角色（用户组）权限申请/变更流程管理流程。通过管理用户的访问权限，保证只有经过授权的用户才可以访问IT系统或服务，以保证业务系统安全运行。

**管理流程：**

帐号、角色（用户组）权限申请/变更管理流程应包含提交申请、审核、执行、确认并归档等功能。

【主要功能点】

* 支持提交人填写申请单，送部门审核人。
* 支持部门审核人如审核通过后，可送业务部门继续审核，也可送帐号管理部门审核。
* 支持部门审核人如审核不通过时，可退回给申请提交人。
* 支持申请提交人收到退回的申请单后，可修改后重新提交，或者直接取消，结束流程。
* 支持业务部门审核通过后，可送帐号管理部门继续审核。
* 支持业务部门申请不通过时，可退回给申请提交人。
* 支持帐号管理部门审核通过后，可送帐号管理部门管理员执行帐号、角色权限变更。
* 支持帐号管理部门管理员确认执行完毕后，可送帐号、角色（用户组）权限申请提交人确认。

支持帐号、角色提交人确认后，可将申请单归档。

### 服务请求管理

服务请求流程是对来自 IT 用户的低风险、低成本的例行请求进行处理的流程，包括服务请求记录、审批、执行、关闭等环节。服务请求如：信息咨询、建议、非系统类投诉、重置密码、桌面服务请求等。

 **管理流程：**

服务请求管理流程是对来自IT用户的低风险、低成本的例行请求进行处理的流程，确保服务请求处理过程中的关键信息能正确记录，为流程持续优化提供准确的数据信息。

【主要功能点】

* 支持报障人以WEB方式登录系统，上传需补充的附件材料，提交表单到服务台坐席。
* 支持服务台坐席可接听请求电话，根据用户请求内容、请求级别等新建请求单，提交事件单给接障人或者接障组，事件来源为：语音电话来源。
* 支持如果服务台回访人确认事件尚未被排除，可重新报障，系统自动将原报障单内容拷贝到重新保障单中，提交表单到服务台二线支持人，继续处理，要求对于重新产生一张事件单，于原单应有关联。
* 支持服务台回访人确认请求已经完成，可关闭请求单，关闭后的请求单需要更新状态，且不能重打开，支持填写处理满意度。
* 支持服务台审核人可接收服务台坐席提交的请求单审核，对请求的重要性批示，可修改请求单项，然后派单给二线支持人员处理。
* 支持服务台审核人可以Email或者短信形式将请求单内容通知责任人。
* 支持在请求单页面随时上传、下载附件。
* 二线支持人登陆系统，查询个人待处理请求单，打开请求单，查看详细信息，判断请求单内容，如不属于自己所在请求处理组处理范围，可转派其他请求处理组或者请求人。
* 支持二线支持人可发短信或者电子邮件通知相关人员。
* 支持二线支持人需外出处理请求时，可编辑派出单内容后，打印派出单。
* 支持服务请求清单导出成EXCEL文件功能。
* 支持后转跟踪单：请求事件若因客观条件需等待长时间才能完成，可在结束事件单时产生后续跟踪单。

### 事件管理

事件管理记录和管理事件从发生到业务恢复的过程，主要包括来自IT基础架构的事件告警、来自客服和业务部门的客户投诉，也包括来自其它业务部门的服务请求。事件管理包括事件发起和记录、事件分派、事件处理、事件确认、事件关闭、统计查询、事件监察等功能。

**管理流程：**

结合“2.1.1故障响应流程及规范”章节实现事件管理包括事件发起和记录、事件分派、事件处理、事件确认、事件关闭、统计查询、事件监察等流程和功能。

#### 事件发起和记录

事件发起功能用于发起一个事件流程实例。事件发起有两种方式：

* 手工发起；
* 通过外接口发起。

事件发起后，事件单数据以及流程流转过程相关数据由系统自动记录。

【主要功能点】

* 支持WEB方式创建事件单；
* 支持随时上传必要的附件信息，附件保存在服务器的附件库中；
* 支持根据用户配置事件等级处理时限规则自动换算事件处理时限；
* 支持报障人联系电话，区域，部门等内容由系统默认填写；
* 事件单表单信息包括对整个流转过程的历史跟踪记录；
* 支持对事件流转的整个流程划分事件单状态；

#### 事件分派

系统支持事件受理人员人工分派和自动分派2种方式，并且可以重新分派。

【主要功能点】

* 用户登录系统后，根据自己的权限可以看到自己应处理的事件单，并且根据角色的不同所看到的表现形式也是不同的；
* 支持向受理人员发出提示信息，如手机短信、电子邮件等，提示及时处理事件单；
* 事件单自动分拣规则支持用户自定义。

#### 事件确认和关闭

事件处理完毕后需由报障人进行确认。报障人根据事件是否解决，关闭事件单或者重新报障。

【主要功能点】

* 当事件流程实例没有完全被完成的时候，不允许无条件的人为结束事件流程。

#### 事件监察

事件监察实现对超时事件单情况的实时统计监察。以图表方式直观展示当前时刻超时事件单数量及详细信息。使用户可以对全部事件单超时情况进行把控

#### 事件通知

系统与短信网管，邮件系统通过接口相互关联，可以向相关人员发送待办信息，手机待办，邮件待办。并在事件单流转的任何阶段，可以向相关人员发出提示信息，如手机短信、电子邮件等。

【主要功能点】

* 短信，手机提示信息内容支持规则配置，系统按照配置规则向用户发送提示信息；
* 是否发送手机待办，邮件待办，支持用户个性化定制。

### 问题管理

问题管理流程是确定某一事件或具有相同症状的一组事件的根本原因，制定和实施解决方案，从而防止事件再次发生的管理流程。问题管理流程的目的是找出事件根本原因，尽可能的给出解决方案或者临时应对措施。包括问题发起和记录、问题分派、问题处理、问题确认、问题确认和关闭、问题相关知识查询、通知及反馈、统计分析、综合查询、考核、规则配置等功能。

### 知识管理

知识管理主要是实现知识管理流程的管理功能，将各个系统运行维护的案例、经验等信息沉淀到一个统一的知识数据库中，使之能够为日常的维护工作提供信息支持。知识管理包括知识录入、知识审批、知识检索和发布、知识库维护等功能。

#### 知识录入

系统支持知识的录入过程，在知识入库之前任意编辑。

【功能要求】

* 支持手工录入，操作员将在各种场景获得的知识录入系统，支持拷贝、粘贴等编辑功能；
* 支持知识分类，可按多种维度分类；
* 支持知识审批入库之前管理员对知识进行任意的编辑修改；
* 支持将知识文档以附件方式添加到知识记录中；
* 支持知识需求的提出，即知识使用者在检索知识库的过程中发现需要的知识并不存在，则可以提出知识需求，并由知识库管理者进行收集、补充。

#### 知识审批

对知识审核队列的知识进行审批，只有审批通过的知识才能进入知识库，成为正式知识。功能要求如下：

【功能要求】

* 支持填写审批意见，自动生成审批人、审批时间等。

#### 知识库维护

对知识内容进行编辑，并定期清除过期的知识，功能要求如下：

【功能要求】

* 支持对知识的编辑修改功能，修改知识的文本、添加分类、增加关键字、添加附件等；
* 支持知识库的删除功能，定期对过期知识进行清除，提供知识记录和附件资料的级联删除功能；
* 支持知识分类的维护。

#### 知识检索和发布

通过知识系统的检索功能，更高效、更方便来提供对知识的定位，并以简洁的方式展示知识。功能要求如下：

【功能要求】

* 支持分类检索和关键字检索；
* 支持其他条件的查找；
* 支持知识的发布，新知识可以以告警、通知等形式发布给相关的用户。

### 日常运维管理

#### 作业计划管理

作业计划管理的主要功能是对IT人员的日常维护作业进行统一管理，运维人员通过制定日常维护作业计划实现维护作业管理。

【主要功能点】

* 系统支持作业计划的制定，作业计划的定制的配置信息，包括作业项目、作业目的、作业计划类型、作业周期、执行人、审核人等；
* 支持多种作业计划：自动执行作业计划、人工执行作业计划；
* 支持定义作业计划模板；
* 支持对作业计划定制权限的限制，只有具有一定权限的工作人员才可以制定作业计划；
* 支持多种作业任务提醒方式：短信或者Email形式；
* 支持作业计划结果的登记，审核管理；
* 支持记录作业计划执行操作人、操作时间、记录操作过程中的相关数据变更，作为历史记录查询的依据；
* 支持作业计划组管理，可以将作业计划按组归类管理；
* 支持按照多种维度查看作业计划执行结果：按作业计划维度，按管理对象维度。

#### 统计分析

利用整合及汇总后的数据，系统自身可直接可提供满足用户业务需求的各种报表。

【主要功能点】

* 支持作业计划处理情况统计报表；
* 支持作业计划自身属性数据统计报表。

### 系统管理

系统管理主要包括用户管理、角色管理、组织管理、权限管理、系统日志管理等，确保IT服务管理系统支持安全有序地运行。

#### 用户管理

用户是指授权访问系统的使用者。用户管理用来记录用户相关信息，如账户、密码等。用户要拥有对某个主题的操作权限，必须通过角色去关联。

【主要功能点】

* 用户名称（ID）在全企业唯一，缺省为员工工号；
* 用户的初始密码由安全管理员设置，统一在系统管理的个人资料录入中完成；
* 安全管理员支持修改用户的密码，统一在系统管理的个人资料修改中完成；
* 各级管理员在本人权限范围内支持对用户进行增加、删除、修改等操作；
* 各级管理员在本人权限范围内支持对用户密码进行修改；
* 用户缺省支持修改本人的密码；用户首次登录后，系统提示用户必须进行密码的修改；
* 对密码的要求：
* 长度要求：6<=密码长度<=16；
* 字符要求：数字、大小写字母、标点符号；
* 复杂性要求：不能包含用户名（不区分大小写）；密码字符必须含有数字、大写字母、小写字母、标点符号四种中的三种字符；
* 变更要求：新密码不得与最近使用的两个密码相同，密码更改的时限可由系统安全管理员设置（缺省：90天）；
* 对密码的加密要求：采用不可逆的加密算法，密码以密文方式存入数据库；密码以密文方式在网上传输。
* 可以对用户进行查询统计。

#### 角色管理

角色就是系统中的一组权限的集合。系统管理员定义系统中的角色、角色适用的部门类型、功能权限集，以方便管理人员对员工进行权限分配。

系统中的每个具有合法使用权限的用户都会被分配一个或数个角色，它是使用权限的基本单位，拥有一定数量的权限，通过角色赋予用户权限。

角色管理的基本操作：进行系统管理员身份认证后，授予用户相应的角色；修改用户的角色，相关的操作结果存入用户\_角色表中；也可以增加角色，相关的操作结果存入角色表中。

【主要功能点】

* 创建角色：当用户所需的角色不在系统原有角色中时，可由系统管理员创建新的角色，以满足用户的需要；
* 授予用户角色：当用户建立好后，要给用户授予适当的角色获取一定的权限；
* 修改用户角色：可以对用户的角色进行重新分配，即修改。角色具有以下主要属性：
	+ 编号：在系统中唯一；
	+ 名称：在系统中唯一；
	+ 注释：描述角色信息。
	+ 可以删除角色；
	+ 可以根据角色进行查询统计。

#### 权限管理

权限指访问系统的用户根据角色获得对系统某些功能的操作，例如读、写、修改和删除等功能。

授权管理的基本操作：进行系统管理员身份认证后，为角色分配相应的权限，修改角色的权限等操作，相关的操作结果存入角色\_权限表中；并可以在模块对象发生变化后，创建对象权限，相关的操作结果存入权限表中。

【主要功能点】

* 支持创建对象权限：当增加系统对象时，创建该对象的权限；
* 支持分配角色权限：给不同的角色分配相应的权限；
* 支持修改角色权限：根据需要，可以修改角色的权限；
* 权限设置必须由被授权的系统管理员完成，管理员不能设置大于自身权限的权限；权限管理采用分级的管理方式。上一级可以设置下一级的管理权限；
* 权限具有以下主要属性：
	+ 编号，在系统中唯一；
	+ 名称，在系统中唯一；
	+ 注释，描述权限信息。
* 权限、角色、用户之间具有如下关系：
	+ 用户与角色的多对多关系

一个用户可以隶属于多个角色，一个角色组也可拥有多个用户，用户角色就是用来描述它们之间隶属关系的对象。用户通过角色关联所拥有对某种资源的权限。

* + 权限与角色的多对多关系

权限是一个二元组关系，包括对象和对对象的操作。对象包括用户操作的系统模块和数据对象，通过权限与角色的关系来设定角色操作对象的权限。一个角色可以拥有多个权限，同样一个权限可分配给多个角色。

#### 组织管理

组织机构包括省、市、县（区）各级各类部门、班、组等。组织管理完成对其按组织结构进行统一编码和维护。

【主要功能点】

* 系统按照组织结构对省、市、县（区）各级各类部门、班、组等进行统一编码，按人员的组织结构从上往下进行管理，具体编码方式和位长可根据实际情况进行编排；
* 具有相应权限的用户可对省、市、县（区）各级各类部门、班、组等进行编码并进行增加、修改、删除等操作，并对上下级关系等进行增加、修改、删除；
* 系统支持组织机构的树状层次管理，一个组织机构可以有多个子节点；
* 可以对编码和组织结构进行查询统计。

#### 系统日志管理

日志管理是对各个关键处理部位采用日志管理的方法，保证网络和IT 服务管理系统的安全、可靠和稳定运行，及时发现、及时预防故障隐患，避免系统运行事故的发生。

【主要功能点】

* 系统登录日志管理
	+ 系统登录日志记录，系统应能将用户的登录信息(包括成功与不成功的登录)记录下来，以供查询。用户登录信息包括用户名称、登录终端名称与IP 地址、登录时间和退出时间。
	+ 系统登录日志查询，系统应能够查询系统登录日志。查询条件包括用户名称、IP 地址、登录日期时间、登录结果（成功或失败）等。查询内容包括用户名称、登录终端名称与IP地址、登录时间和退出时间。
	+ 系统登录日志删除，系统应能够删除过时的系统登录日志。系统应提供以下两种删除方式，一是按时间进行删除；二是按保留的记录条数进行删除。
	+ 系统登录日志备份，系统应具有自动备份系统登录日志到硬盘和手动保存系统登录日志到Excel文件的功能。系统应具有打印系统登录日志功能。
* 系统操作日志管理
	+ 系统操作日志记录，系统应能将用户的操作信息记录下来，以供查询。操作信息包括实施操作的用户、操作时间、IP 地址、操作名称、操作对象、操作结果。
	+ 系统操作日志查询，系统应能够查询系统操作日志。查询条件包括用户名称、IP 地址、操作日期时间、操作结果（成功或失败）等。查询内容包括实施操作的用户、操作时间、IP 地址、操作名称、操作对象、操作结果。系统应具备模糊查询方式。
	+ 系统操作日志删除，系统应能够删除过时的系统操作日志。系统应提供以下两种删除方式，一是按时间进行删除；二是按保留的记录条数进行删除。
	+ 系统操作日志备份，自动备份系统操作日志到指定设备和手动保存系统操作日志到Excel 文件的功能。系统应具有打印系统操作日志功能。

#### 流程引擎

流程引擎是支撑业务管理流程的基础。包括流程定义、流程启动、流程控制、流程监控、流程查询等功能。

* 流程定义

流程定义提供一个可以定义各类流程模板的工具。支持直观的、可视化的、灵活方便的流程模板配置和展示界面。流程模板由环节模板和路径模板构成。

* 流程启动

流程启动有通过Web方式启动和业务驱动启动2种方式，功能要求如下：

【主要功能点】

* + 支持通过Web方式启动流程：对于业务依赖性很小的流程，可以由操作员通过Web界面启动流程。流程启动之后依据模板定义好的路径逻辑，系统将判断是否需要由用户手工创建下一环节，如果需要则提示用户进入下一环节的创建界面，否则，系统将自动创建下一环节；
	+ 支持业务驱动启动流程：许多流程是由于业务触发启动的，因此相应的业务功能模块要通过调用流程引擎的后台驱动函数启动流程。
* 流转控制

流转控制控制流程的实例运转，产生员工的任务工单。功能要求日下：

【主要功能点】

* + 支持正常流转：表示流程的正常向后流转，即用户选择“完成”的情况；
	+ 支持回退：流程往后流转，即用户选择“回退“的情况；
	+ 支持转办：表示用户操作时请求其他用户协同办理。即用户选择“转办“的情况。转办的时候环节实例表的状态不会改变；
	+ 支持撤回：当流程实例的当前实例尚未被“执行“时，前面环节的用户可以撤回；
	+ 支持接收：对于共享任务和非必办任务体供“接收“功能，共享任务一旦接收则其他用户不能办理，非必办任务一旦接收，变成必办。
* 流程监控

流程监控是对流程运行实例的运行情况的监视和分析手段之一。功能要求如下：

【主要功能点】

* + 统计分析可针对某一个流程实例进行，也可以对基于同一模板的某一类流程进行；
	+ 支持针对流程执行时长，执行人员数和执行数量及超时时长，超时数量等指标的统计分析。
* 流程查询

流程查询是对流程运行实例信息的查询，它包含流程实例查询和流程中各环节实例的查询。

对于一些常用的流程，需要有专门的流程管理页面，集合了上述流程查询、创建、执行等功能。用户可以通过选择不同查询条件查找所关心的流程，或者启动新流程。

#### 接口管理

按需可对接各类业务系统实现流程的发起、自动流转、手动流转等功能。

## ITMP监控系统

监控系统主旨建立统一的监控管理，监控采集，监控分析，监控告警，监控汇报的监控系统对监控设备进行不间断的实时监控，主要目的在于发现故障的第一时间及时通报相关人员，以此减轻甚至减免故障导致的不良影响。系统提供各种维度的管理功能，使运维体系的监控数据易管理，易维护，易扩展；系统提供多元的监控类型支持，多样的采集手段，使运维体系的监控范围更广；系统提供统一的告警处理，使运维体系中故障处理更加集中，更加高效，更加精准。除了及时发现故障，通报故障，处理故障，监控系统所产生的日常监控数据的汇总，亦可对整个运维体系的调整，扩展提供实质的数据参考作用。

### 监控管理

系统提供图形化管理界面管理监控相关的各种信息，对于运维体系的监控设备信息，可通过系统的监控对象管理，按照该系统提供的管理方案对所有录入的监控设备进行分类归纳管理，使监控设备数量再庞大亦可控，可维护；对于运维体系的监控精度，可通过采集规则管理，告警分析规则管理，将监控精确控制到某一指标，时间的某一刻度，加强运维监控的力度；对于运维体系的监控故障响应效率，通过告警通知规则管理，将故障信息简要明确及时的通知到相关的人员，使故障能尽快地被知晓，被处理。

* **监控对象管理：**系统提供统一的监控对象管理功能，系统会根据“地区-所属系统-所属监控类型”逐级将监控对象归纳组成监控对象树，管理方便运维人员查询管理。
* **采集规则管理：**系统提供采集规则配置管理页面，用户可针对不同类型的监控对象，对其配置该类型特有的监控指标，并且逐项的监控指标可配置特定的采集频率，频率精度可精确到秒级，实现个性化的灵活配置的同时，系统支持已经配置完成的指标可抽象为模板下发于其他监控对象，减少配置重复繁重的工作量。
* **告警分析规则管理：**系统支持针对逐项的监控指标指定特定的告警阈值规则，并且可设置多阈值，对于不同的阈值范围定义为不同级别的等级告警，系统支持已经配置完成的告警阈值可抽象为模板下发于其他监控对象，减少配置重复繁重的工作量。
* **告警通知管理：**系统支持维护人员通过控制“告警等级，通知时间，监控对象，通知模板，相关人员“等维度进行告警通知管理。

### 监控采集

系统支持主机系统、数据库、中间件、网络设备、应用、业务的性能指标采集。支持SSH、TELNET、SNMP、ICMP、SYSLOG、JDBC、SCOKET，HTTP等采集方式。系统支持多样化的采集手段，支持多元化的监控类型，为整个运维体系能监控并维护绝大部分的监控设备创造必要的条件，使整个运维体系可监控，可运维的范围更广。

* **主机监控**：支持对HP-Unix、Solaris、Linux、AIX、Windows等主流操作系统的监控。指标包括但不限于CPU使用率、总内存大小、物理内存使用量、物理内存使用率、虚拟内存使用率、虚拟内存使用量、磁盘使用率、磁盘分区总空间、磁盘剩余空间、每秒IO写速率、每秒IO读速率、IO队列长度、指定文件的大小、指定文件的增速、总进程数目、进行资源占用等。
* **网络设备监控**：支持自动发现和手动添加两种方式监控网络设备，可支持市场上常见的厂家路由器、交换机、安全设备、负载均衡等设备的性能指标采集和预警。指标包括但不限于在线状态、Ping延时、CPU、内存、端口状态、逻辑链路（Eth-trunk）状态、端口速率、端口带宽利用率、端口丢包率、端口错包率等。
* **数据库监控**：支持Oracle、MySQL、SQLServer、DB2等各类关系型数据库的监控。指标包括：数据库负载与状态、数据库表空间、数据库内存、数据库会话、数据库锁、错误日志、rman告警条数，监听状态，数据库服务器top信息记录，高占用SQL、会话详情等。
* **中间件监控**：支持市场上各类主流应用服务器及中间件的信息监测，至少包括WebSphere、Weblogic、TOMCAT、Tuxedo等中间件。提供包括基本信息、连接池、线程队列、负载监测、通道情况监测等多类监测指标。
* **应用监控：**支持对于用户指定的特定应用接口进行定时请求或页面访问，从而监控应用是否正常运行。
* **业务监控：**支持对于用户自定义脚本对于特定的数据库数据进行查询，或服务器的特定数据进行脚本查询，从而实现用户自定义的脚本监控目的。

### 监控分析

系统支持数字，字符串关键字分析，提高运维体系监控分析的实用性；多样的数据分析接入，通过统一的分析引擎得出统一的等级分明的告警结果，为运维体系中，监控后续的故障处理提供一个统一标准参考。

* **数字阈值分析**：系统支持对采集到的数据进行数字阈值判断，按照用户配置分析出监控指标是否需要进行告警。
* **字符串关键字分析**：系统支持对采集到的数据进行字符串关键字匹配判断，按照用户配置分析出监控指标是否需要进行告警。
* **告警级别分类**：上述告警分析都支持将告警按用户配置的告警规则，按严重性分类为：严重，主要，次要。同时系统会将告警分为系统告警（由系统维护人员负责处理修复），阈值告警（由业务人员或设备负责人进行核查并且处理）。

### 监控告警

系统提供统一的告警展示，统一的告警处理维护，以及统一的告警质量优化，在运维体系中，使故障处理更加集中，更加高效，更加精准。

* **告警统一展示**：系统提供统一的告警大屏展示，维护人员可在告警台对告警进行统一处理，同时告警台支持不同维度的过滤展示辅助维护人员处理告警。
* **告警处理**：系统支持图形化处理告警，包括的处理动作有告警过滤、告警确认、告警清除、告警派单等操作。
* **告警质量优化：**系统支持预定义部分告警或预定义部分规则，在告警的分析和产生的过程中对于部分告警进行屏蔽，压缩，吸收，减少告警的数据量，提高告警的质量

### 监控汇报

监控系统可向运维体系，提供日常的监控数据而形成的报表，描述性能的趋势走向，描述体系中不同监控设备，不同时间段的性能对比，描述日常的告警汇总情况，为运维体系的调整，扩展提供实质的数据参考作用。

* **单指标报表**：针对每个监控对象，都有其针对单个性能指标的性能数据曲线图的报表查询。
* **自定义报表**：系统支持用户自定义报表生成，用户可通过控制“监控对象”，“监控指标”，“监控时间”等维度按自身需求定义报表生成规则，生成特定的性能数据汇总报表或性能数据比较报表。
* **告警汇总**：系统每天都会根据不同的告警等级作为统计维度统计每天产生的不同等级的报表并制成曲线图在系统展示

### 告警应用：对接工单系统

监控系统获取到的告警数据，能够通过实时接口触发工单系统实现建单、派单功能，从而实现告警从产生到消除的有效的闭环处理。

## CMDB系统

### 生命周期管理

管理服务器类设备从入库到报废的全生命周期状态，为优化企业资源配置提供决策支持信息。

#### 批量处理

批量导入&修改设备的基础配置信息，设备归属信息，关联配置信息，业务归属信息。

【主要功能点】

* 下载批量处理模板
* 导入数据校验，按模板中的数据字典与预配置的校验规则，校验输入信息的有效性。
* 导出校验错误信息，提供精确到行列的错误提示。
* 按配置项模型生成设备配置项属性与关联关系。
* 批量新建&修改设备生命周期状态，设备归属，业务归属。
* 按查询条件导出设备信息。

#### 历史记录管理

设备每次信息变更，都会有主记录，记录变更时间，变更人，变更原因，本次变更信息字段变更前和变更后的内容会记录在变更详情记录中。管理人员可以按条件导出变更记录主表与详情，进行设备变更统计分析。

#### 下架管理

 设备生命周期状态变更为【已下架】后，在生命周期管理详情中会自动过滤该条记录。管理员可以在下架管理中查询到该条记录，查询&导出该条设备的详情信息，变更历史记录。

### 网络设备与IP段管理

管理实物系统中的网络设备与IP段的信息。

 【主要功能点】

* 展示与查询网络设备与IP网段信息
* 新增&修改&删除&导出IP网段信息
* 批量导入&导出IP地址信息。
* 新增&修改IP地址分配信息
* IP回收和再分配。
* 查看IP地址分配回收记录操作历史记录。

### 资源利用率管理

 定时从监控系统同步资源性能统计信息，关联CMDB中的配置项信息，生成设备平均利用率记录，管理员可以导出&查询月资源利用率报表，日平均利用率报表。

### 配置项管理

对实物管理模块的配置项属性进行统一管理，提供配置项属性查询、展示入口，按运维需求对配置项属性进行自定义配置。

【主要功能点】

* 配置项树结构生成。
* 配置项属性的展示与查询
* 配置项关联关系管理
* 配置项资源展示与查询
* 配置项拓扑视图

### 数据字典管理

数据字典模块主要对平台所需选项数据进行管理，整个数据字典数据为平台所共享，管理员可灵活控制CMDB中的下拉可选数据（比如生命周期状态，规格型号等），提高数据灵活性。