智慧工业园区大数据云平台

建设方案

目录

第一章 项目建设背景及现状 24

1.1. 项目建设背景 24

1.2. 项目建设必要性 25

1.3. 项目建设目标 26

1.4. 建设原则 26

第二章 园区创新发展趋势 28

2.1 园区经济向生态型转变 28

2.2 园区企业向高新型转变 29

2.3 园区管理向城市化转变 29

第三章 工业园区大数据存在的问题 29

3.1 信息化配套设施及服务不够完善 29

3.2 信息资源整合利用工作严重滞后 30

3.3 智慧化推进工作缺乏有效抓手 30

3.4 园区综合管理缺乏智能化手段 31

3.5 节能环保新技术应用匮乏 31

第四章 智慧工业园区大数据建设目的 31

4.1 智慧化提升园区吸引力 31

4.2 智慧化促进园区可持续发展 32

4.3 智慧化助力园区发展战略性新兴产业 32

4.4 智慧化顺应信息技术创新与应用趋势 32

第五章 智慧园区总体构架 33

5.1 新一代信息基础设施 34

5.2 集约共享的信息资源利用体系 35

5.3 智慧应用体系 36

5.4 智慧园区安全体系 37

5.5 智慧园区管理体系 37
第六章 系统核心组件 39
6.1 系统总体设计 39
6.2 系统网络架构设计 41
6.3 底层消息交互组件 42
6.3.1 消息服务机制 42
6.3.2MQ 的主要特点 43
6.4 多媒体融合通信服 44
6.5 电子地图服务 44
6.5.1 基础图层数据服务 44
6.5.2 地图空间图层数据查询服务 44
6.5.3 实现地图上应用基本功能 45
6.6 运行维护管理 45
6.6.1 组织机构管理 45
6.6.2 系统用户管理 45
6.6.3 系统权限管理 46
6.6.4 系统角色管理 46
6.6.5 系统日志管理 46
6.7 系统用户管理 46
6.8 智工业园区社会综合治理云平台综合态势展示 46
6.8.1 智工业园区治安防控情报信息上报汇总 47
6.8.2 智工业园区群防群治勤务运行信息 47
6.8.3 社会化治安防控实战指挥态势图 47
6.8.4 宏观预警及趋势分析 47
第七章 智慧工业园区大数据平台规划设计 48
7.1 需求分析 48

7.1 .1 采购范围与基本要求 48
7.1.2 建设内容要求 48
7.1.2.1 人口库 48
7.1.2.2 法人库 48
7.1.2.3 地理信息库 49
7.1.2.4 视频库 49
7.1.2.5 大数据处理平台 49
7.1.2.6 数据管理服务平台 55
7.2 设计方案 58
7.2.1 总体平台设计 58
7.2.1.1 总体架构 58
7.2.1.2 体系结构图 58
7.2.1.3 总体流程图 58
7.2.2 人口基础数据库设计 59
7.2.2.1 数据接收服务 59
7.2.2.2 中心数据查询 59
7.2.2.3 决策支持子系统 60
7.2.2.4 授权管理 60
7.2.2.5 设计方案 60
7.2.2.6 信息核验 60
7.2.2.7 系统管理 60
7.2.3 法人基础数据库设计 61
7.2.3.1 系统管理 61
7.2.3.2 授权服务 61
7.2.3.3 接收服务 61
7.2.4 信息服务 62

7.2.3.5 统计分析 62
7.2.3.6 地理信息基础数据库设计 62
7.2.3.7 基础数据 62
7.2.3.8 平台建设 64
7.2.3.9 GIS 平台 69
7.2.4 视频基础数据库设计 72
7.2.4.1 建设规划 72
7.2.4.2 设计方案 73
7.2.5 大数据处理平台 74
7.2.5.1 大数据处理平台 74
7.2.5.2 大数据多维分析查询系统 81
7.2.5.3 大数据智能分析系统 87
7.2.6 数据管理服务平台 89
7.2.6.1 数据治理与监控系统 90
7.2.6.2 数据服务集成管理系统 95
7.2.6.3 大数据展现门户 100
7.3 实施方案 103
7.3.1 项目组织实施 103
7.3.2 突发事件处置 105
7.3.3 项目验收 106
7.3.4 项目交付 107
7.3.5 项目管理与质量保障 107
第八章 智工业园区治安防控情报信息上报 112
8.1 社会化警务助理信息上报 112
8.2 信息图上展现 112
8.3 服务管理对象定位信息管理 112

8.4 服务管理对象定位上图 113
8.5 视频监控集成接入网关（可选） 113
8.6 图上周边资源查询 113
8.7 通知公告 113
8.8 逐级精细管理模式 113
8.9 事件上报 114
8.10 平台事件自动分流 114
8.11 绩效自动考核 114
8.12 事件项目可定制 114
8.13 接口开放 114
8.14 GIS 可视化操作 114
8.15 符合规范 115
第九章 服务管理对象一键报警（可选） 116
9.1 服务管理对象互联网 APP 端一键报警 116
9.2 警情进入三台合一接处警 116
9.3 警情状态更改 116
9.4 辖区手动扁平派警 116
9.5 图上就近扁平调警 116
9.6 警情警力实时态势 117
9.7 人口管理 117
9.8 特定人口管理 117
9.9 单位法人管理 117
9.10 XXX 区社区单位管理 117
9.11 商户管理 118
9.12 民情上报 118
9.13 警情上报 118

9.14 自动考核.....118
9.15 自动统计.....119
9.16 自动通知.....119
9.17 自动催促.....119
9.18 流程定制.....119
9.19 事件定位.....119
9.20 人口定位.....119
9.21 事件流程跟踪.....119
9.22 分级管理.....120
9.16 自动通知.....120
9.23 老人和儿童管理.....120
9.24 公共安全管理.....120
9.25 邻里矛盾解决.....120
9.26 舆情监控.....120
9.27 XXX 区社区环境监控.....120
9.28 黄赌毒及时发现.....121
9.29 邪教组织及时发现.....121
9.30 公共设施管理.....121
9.31 志愿者管理.....121
第十章 社会化治安防控力量实战指挥.....122
10.1 指挥调度及警令流程.....122
10.2 智能堵控圈.....122
10.3 一键“关城门”.....122
10.4 指挥过程全流程管理.....122
10.5 总体架构.....123
10.6 XXX 区社区信息数据库.....123

10.7 信息数据管理平台 124
10.8 物业管理平台 124
10.9 园区服务审批平台 126
10.10 XXX 区社区商务缴费平台 127
10.11 医疗服务平台 128
10.12 信息发布平台 128
10.13 园区管理平台 128
第十一章 园区管理平台 130
11.1 勤务资源库管理 130
11.1 勤务资源库管理 130
11.1 勤务资源库管理 130
11.1 勤务资源库管理 130
11.1 勤务资源库管理 130
11.1 勤务资源库管理 130
11.1 勤务资源库管理 130
11.1 勤务资源库管理 130
11.1 勤务资源库管理 130
11.1 勤务资源库管理 131
11.2 值班备勤 131
11.3 巡防报备 131
11.4 专项任务勤务报备 131
11.5 勤务查询 131
11.6 勤务监督 131
11.7 绩效统计 132
第十二章 服务管理对象互联网 APP 133
12.1 治安防控信息上报 133
12.2 我的上报历史信息 133

12.3 我的任务 133
12.4 工作任务反馈录入 133
12.5 警务即时通信 133
12.6 警务通讯录 134
12.7 现场取证多媒体资料回传 134
12.8 一键报警 134
12.9 通知公告 134
12.10 审批 134
12.11 勤务数据分析 134
第十三章 智慧工业园区云平台建设 135
13.1 总体建设方案 135
13.1.1 智慧园区大数据云总体架构 135
13.1.2 数据中心间互联架构 135
13.1.3 云服务商平台总体架构 136
13.1.4 智慧园区大数据云总体网络拓扑设计 136
13.1.4.1 现有数据中心改造 136
13.1.4.2 现有数据中心、A 中心和 B 中心连接设计 137
13.1.5.1 xxx 网安全拓扑设计 138
13.1.5.2 互联网安全拓扑设计 139
13.1.6 云管理平台架构设计 139
13.1.6.1 IT 架构面临的问题 139
13.1.6.2 云平台架构新思考 140
13.1.6.3 VCF 虚拟融合架构 142
13.1.6.4 VCF 架构下的云平台 143
13.1.6.5 云平台融合架构设计 143
13.1.7 xxx 网云平台方案 144

13.1.7.1 基础架构层 144
13.1.7.1.1 设备选型 145
13.1.7.1.2 专享业务区 148
13.1.7.1.3 管理和服务区 149
13.1.7.1.4 云数据库区 149
13.1.7.1.5 安全访问区 150
13.1.7.2 资源融合控制层 151
13.1.7.2.1 融合控制体系 151
13.1.7.2.2 网络控制器 151
13.1.7.2.3 虚拟化管理平台 152
13.1.7.2.4 计算资源池构建 153
13.1.7.3 云服务及资源管理层 157
13.1.7.3.1 IaaS 服务 157
13.1.7.3.2 PaaS 服务 158
13.1.7.3.3 多租户组织架构 159
13.1.7.3.4 委办局云服务使用流程 159
13.1.7.3.5 云服务的申请与审批 159
13.1.7.3.6 云服务交付 159
13.1.7.4 vDC 虚拟数据中心 165
13.1.7.4 vDC 虚拟数据中心 165
13.1.7.4 vDC 虚拟数据中心 165
13.1.7.4 vDC 虚拟数据中心 165
13.1.7.4 vDC 虚拟数据中心 165
13.1.7.4 vDC 虚拟数据中心 165
13.1.7.4 vDC 虚拟数据中心 165
13.1.7.4 vDC 虚拟数据中心 165

13.1.7.4 vDC 虚拟数据中心 166
13.1.7.4 vDC 虚拟数据中心 166
13.1.8 互联网云平台架构 169
13.1.9 云平台部署逻辑架构 170
13.2 IaaS 层方案 170
13.2.1 网络虚拟化 170
13.2.1.1 基本需求 170
13.2.1.2 技术选择 170
13.2.1.3 模型选择 171
13.2.1.4 SDN 网络规划与设计 173
13.2.1.5 Overlay 网络介绍 174
13.2.2 安全虚拟化 178
13.2.2.1 安全网关虚拟化 178
13.2.2.2 虚拟化架构 - 横向及纵向扩展性 180
13.2.2.3 虚拟化架构 -1 :N:M 虚拟化 180
13.2.2.4 虚拟化架构 - 接口共享虚拟化 180
13.2.2.5 虚拟化架构 -N:1 虚拟化 181
13.2.2.6 安全功能虚拟化 - 虚拟软件安全网关 183
13.2.2.7 安全虚拟化与安全服务 184
13.2.2.8 采用服务方式的安全控制 187
13.2.3 计算虚拟化 188
13.2.3.1 虚拟化资源池 188
13.2.3.2 虚拟化安全隔离 188
13.2.3.3 虚拟机/ 存储热迁移 189
13.2.3.4 虚拟机高可靠 HA 189
13.2.3.5 虚拟机规格动态调整 189

13.2.3.6 自动化弹性调度 190
13.2.4 存储虚拟化 190
13.2.4.1 集中式存储规划设计 191
13.2.4.2 分布式存储规划设计 192
13.2.5 整体关键技术虚 201
13.2.5.1 网络虚拟化技术设计 201
13.2.5.2 服务器高可用技术设计 202
13.2.5.3 数据库高兼容性设计 205
13.2.5.4 存储高可用技术设计 206
13.2.5.5 KVM 虚拟技术设计 206
13.3 IaaS 云服务方案 208
13.3.1 IaaS 云服务目录 208
13.3.1.1 计算存储网络服务目录 208
13.3.1.2 安全服务目录 208
13.3.2 云主机服务 208
13.3.2.1 云主机概述 208
13.3.2.2 云主机租户网络 209
13.3.2. 自定义镜像 209
13.3.2.4 云主机特点 210
13.3.3 云硬盘服务 210
13.3.4 云存储服务 210
13.3.4.1 云存储概述 210
13.3.4.2 云存储特性 211
13.3.4.3 云存储接口 API 211
13.3.5 云数据库服务 211
13.3.5.1 云数据库服务介绍 211

13.3.5.2 云数据库服务使用流程 212
13.3.5.3 云数据库服务技术架构 213
13.3.5.4 云服务自动化平台 213
13.3.5.5 技术优势 214
13.3.5.6 数据库性能 214
13.3.6 云防火墙服务 215
13.3.6.1 技术特性 215
13.3.6.2 安全策略 215
13.3.6.3 技术优势 216
13.3.7 云负载均衡服务 217
13.3.7.1 技术特性 217
13.3.7.2 负载均衡策略 217
13.3.7.3 技术优势 218
13.3.8 云入侵防御服务 218
13.3.8.1 技术特性 218
13.3.8.2 入侵防御策略 219
13.3.8.3 技术优势 220
13.3.9 云 WEB 防护服务 221
13.3.9.1 WEB 应用安全防护需求 221
13.3.9.2 WEB 应用安全防护技术 222
13.3.9.3 WEB 防护策略 223
13.3.9.4 技术优势 223
13.3.10 云防病毒服务 224
13.3.10.1 防病毒管理 224
13.3.10.1.1 云查杀检测引擎 225
13.3.10.1.2 人工智能检测引擎 226

13.3.10.2 虚拟机安全防护 226
13.3.10.3 宿主机安全防护 227
13.3.10.4 安全策略管理 227
13.3.11 云安全增值服务 227
13.3.11.1 流量清洗 227
13.3.11.2 安全日志审计 228
13.3.12 云备份服务 229
13.3.13 VPC 服务 230
13.3.13.1 虚拟私有云 (VPC)架构的特点 230
13.3.13.2 虚拟私有云 (VPC)的实现方式 231
13.4 PaaS 层规划设计 232
13.4.1 PaaS 概述 232
13.4.2 PaaS 建设内容 233
13.4.3 PaaS 服务 233
13.4.4 PaaS 优势 234
13.5 云管理平台 234
13.5.1 云管理平台整体架构 234
13.5.2 设备管理 235
13.5.2.1 网络管理 235
13.5.2.2 安全管理 237
13.5.2.3 服务器管理 238
13.5.2.4 存储管理 239
13.5.3 资源管理 241
13.5.3.1 IP 资源管理 241
13.5.3.2 主机应用管理 242
13.5.3.3 服务健康管理 243

13.5.3.4 数据库管理.....243
13.5.4 资源编排.....244
13.5.4.1 网络资源池化.....244
13.5.4.2 网络域和租户管理.....244
13.5.4.3 基于业务的可视化服务编排.....244
13.5.4.4 服务快速申请与撤销.....245
13.5.4.5 全面的服务监控.....246
13.5.5 资源监控.....246
13.5.6 用户管理.....248
13.5.6.1 用户管理策略.....248
13.5.6.2 用户权限控制.....248
13.5.7 流程管理.....249
13.5.7.1 智慧园区大数据云开通流程.....249
13.5.7.2 实时精确的联合 CMDB.....249
13.5.7.3 完整的服务运维流程.....249
13.5.7.4 故障维护流程.....249
13.5.7.5 变更流程.....249
13.5.7.6 流程定制.....250
13.5.7.7 知识库管理.....250
13.5.7.8 服务台.....250
13.5.8 日志管理.....250
13.5.8.1 操作日志管理.....250
13.5.8.2 SYSLog 日志管理.....251
13.5.9 报表管理.....251
13.5.10 计费策略管理.....252
13.6 云安全体系.....253

13.6.1 云平台安全建设要求.....253
13.6.2 智慧园区大数据云平台安全标准要求.....253
13.6.3 等级保护重点要求及分解应对措施等保内容 应对措施.....254
13.6.4 云安全体系架构设计.....259
13.6.4.1 云整体安全逻辑架构.....259
13.6.4.2 云整体安全设计架构图.....259
13.6.4.3 云计算物理层安全.....259
13.6.4.4 虚拟化资源层安全.....260
13.6.4.5 多租户 IaaS 服务层安全.....260
13.6.4.6 PaaS/SaaS 应用层数据安全.....261
13.6.5 各功能区域架构设计.....261
13.6.5.1 核心交换区.....261
13.6.5.2 互联网出口区.....262
13.6.5.3 云管理区.....262
13.6.5.4 数据库系统区.....263
13.6.5.5 东西向资源池区.....263
13.6.5.6 虚拟主机安全防护.....264
13.7 云安全建设方案.....264
13.7.1 物理安全.....264
13.7.1.1 供配电系统.....264
13.7.1.2 防雷接地.....264
13.7.1.3 消防报警及自动灭火.....265
13.7.1.4 门禁.....265
13.7.1.5 保安监控.....265
13.7.2 网络安全.....265
13.7.2.1 网络边界安全.....265

13.7.2.2 防火墙 266
13.7.2.2.1 功能设计 266
13.7.2.2.2 部署设计 266
13.7.2.3 抗拒绝服务攻击（ DDOS 攻击） 设计 267
13.7.2.3.1 功能设计 267
13.7.2.3.2 部署设计 267
13.7.2.4 VPN 安全接入设计 268
13.7.2.4.1 功能设计 268
13.7.2.4.2 部署设计 268
13.7.2.5 网络漏洞扫描设计 268
13.7.2.5.1 功能设计 269
13.7.2.5.2 部署设计 269
13.7.2.6 负载均衡设计 270
13.7.2.6.1 功能设计 270
13.7.2.6.2 部署设计 270
13.7.2.7 入侵防护系统设计 270
13.7.2.7.1 功能设计 270
13.7.2.7.2 部署设计 271
13.7.2.8 网络安全审计设计 271
13.7.2.8.1 功能设计 271
13.7.2.8.2 部署设计 272
13.7.2.9 跨网安全设计 272
13.7.2.10 功能设计 272
13.7.2.11 部署设计 273
13.7.3 主机安全 273
13.7.3.1 主机访问控制设计 273

13.7.3.1.1 功能设计 273
13.7.3.1.2 部署设计 274
13.7.3.2 主机防病毒设计 274
13.7.3.2.1 功能设计 274
13.7.3.2.2 部署设计 274
13.7.3.3 主机安全审计系统设计 274
13.7.3.3.1 功能设计 274
13.7.3.3.2 部署设计 275
13.7.4 虚拟化安全 275
13.7.4.1 虚拟机访问控制设计 275
13.7.41.1 虚拟机访问控制设计 275
13.7.4.1.2 部署设计 276
13.7.5 应用安全 277
13.7.5.1 应用漏洞扫描设计 277
13.7.5.1.1 功能设计 277
13.7.5.1.2 部署设计 277
13.7.5.2 WEB 应用防护设计 278
13.7.5.2.1 功能设计 278
13.7.5.2.2 部署设计 278
13.7.5.3 网页防篡改设计 279
13.7.5.3.1 功能设计 279
13.7.5.3.2 部署设计 279
13.7.5.4 网络架构安全 280
13.7.6 数据安全 280
13.7.6.1 功能设计 280
13.7.6.2 部署设计 280

13.7.7 管理安全.....281
13.7.7.1 安全管理机构.....281
13.7.7.2 安全管理制度.....282
13.7.7.3 人员安全管理.....283
13.7.7.4 系统建设管理.....283
13.7.7.4.1 系统定级.....283
13.7.7.4.2 系统备案.....284
13.7.7.4.3 安全方案设计.....284
13.7.7.4.4 产品采购.....284
13.7.7.4.5 自行软件开发.....284
13.7.7.4.6 外包软件开发.....285
13.7.7.4.7 工程实施.....285
13.7.7.4.8 测试验收.....285
13.7.7.4.9 系统交付.....285
13.7.7.4.10 安全测评.....286
13.7.7.5 系统运维管理.....286
13.7.7.5.1 环境管理.....286
13.7.7.5.2 资产管理.....286
13.7.7.5.3 介质管理.....286
13.7.7.5.4 设备管理.....287
13.7.7.5.5 监控管理.....287
13.7.7.5.6 网络安全管理.....287
13.7.7.5.7 系统安全管理.....288
13.7.7.5.8 恶意代码防范管理.....289
13.7.7.5.9 密码管理.....289
13.7.7.5.10 变更管理.....289

13.7.7.5.11 备份与恢复管理 289
13.7.7.5.12 安全事件处置 290
13.7.7.5.13 应急预案管理 290
13.7.8 安全服务 290
13.7.8.1 安全评测服务 291
13.7.8.2 安全检测服务 291
13.7.8.3 系统漏洞检测服务 291
13.7.8.4 Web 漏洞检测服务 291
13.7.8.5 配置核查服务 291
13.7.8.6 渗透测试服务 292
13.7.8.7 安全评估服务 292
13.7.8.8 重点安全保障服务 292
13.7.8.9 安全培训服务 292
13.8 容灾备份方案 293
13.8.1 容灾数据复制技术 293
13.8.1.1 存储级数据容灾技术 293
13.8.1.2 卷管理级数据容灾技术 293
13.8.1.3 虚拟化级数据容灾技术 294
13.8.1.4 数据库级数据容灾技术 294
13.8.1.5 应用级数据容灾技术 295
13.8.2 容灾整体方案架构 295
13.8.2.1 数据备份 296
13.8.2.2 容灾备份 297
13.8.2.3 容灾方案配置 297
13.8.2.4 本地备份方案 297
13.8.2.5 同城灾备方案 298

13.8.2.6 异地灾备方案 298
13.8.2.6.1 关键业务数据灾备方案 298
13.8.2.7 数据库备份 299
13.8.2.7.1 数据库逻辑备份 299
13.8.2.7.2 数据库热备 - 集群方案 299
13.8.2.7.3 数据库复制 300
13.8.2.8 备份策略 300
13.8.3 数据容灾备份方案 300
13.8.3.1 数据级容灾备份方案 300
13.8.3.1.1 一般数据备份技术架构 300
13.8.3.1.2 关键数据备份技术架构 301
13.8.3.2 应用级主备灾备方案 301
13.8.3.2.1 虚拟化平台容灾技术架构 301
13.8.3.2.2 虚拟化平台容灾实现 302
13.8.3.2.3 业务容灾实现流程 303
13.8.3.2.4 数据库系统容灾技术架构 304
13.8.3.2.5 分布式存储容灾实现设计 305
13.8.3.3 XX 智慧园区大数据云备份方案 305
13.9 云管理平台相关接口及功能 306
13.9.1 云管理平台 API 清单 306
13.9.1.1 用户管理 306
13.9.1.2 网络故障管理 306
13.9.1.3 网络性能管理 307
13.9.1.4 服务运维管理 307
13.9.1.5 云业务管理 308
13.9.2 虚拟化 API 清单 310

13.9.2.1 主机管理 310
13.9.2.2 虚拟机管理 310
13.9.2.3 虚拟机模板管理 311
13.9.2.4 存储管理 311
13.9.2.5 网络策略模板管理 312
13.9.2.6 告警管理 312
13.9.2.7 任务消息管理 312
13.9.3 SDN 控制器 API 清单 312
13.9.3.1 认证管理 312
13.9.3.2 诊断日志 312
13.9.3.3 操作日志 312
13.9.3.4 系统日志 313
13.9.3.5 集群 313
13.9.3.6 Region 313
13.9.3. 313
13.9.3.7 系统信息 313
13.9.3.8 组件配置 314
13.9.3.9 用户配置 314
13.9.3.10 免认证管理 314
13.9.3.11 统计 314
13.9.3.12 应用程序管理 314
13.9.3.13 支持报告 315
13.9.3.14 路管理 315
13.9.3.15 拓扑时间戳 315
13.9.3.16 连通性检测 315
13.9.3.17 设备管理 315

13.10 云监管平台 316
13.10.1 资源监管 316
13.10.1.1 应用管理 316
13.10.1.2 虚拟机管理 317
13.10.1.3 物理机管理 317
13.10.1.4 存储管理 317
13.10.1.5 网络管理 318
13.10.1.6 安全管理 318
13.10.1.7 机房管理 318
13.10.1.8 硬件准入管理 318
13.10.2 接口管理 318
13.10.3 运维管理 318
13.10.3.1 流程管理 318
13.10.3.2 监控告警管理 319
13.10.3.2.1 活动告警 319
13.10.3.2.2 历史告警 319
13.10.3.2.3 活动故障 319
13.10.3.2.4 历史故障 319
13.10.3.3 系统消息提醒 320
13.10.3.4 运维统计报表 320
13.10.3.5 大屏全景展示界面 **错误！未定义书签。**
13.10.3.2. **错误！未定义书签。**
13.10.3.2. **错误！未定义书签。**
13.10.1. **错误！未定义书签。**

第一章 项目建设背景及现状

1.1.项目建设背景

智慧工业园区 PPP 模式有助于弥补县域资源匮乏带来的发展短板,为高质量县域发展提供强大可持续的新动能“完善区域发展政策,推进基本公共服务均等化,逐步缩小城乡区域差距,把各地比较优势和潜力充分发挥出来。” 这是今年政府工作报告对区域协调发展战略的最新部署。

“过去若干年,促进区域协调发展成为中国特色社会主义实践中最具力度、最为生动的内容之一,但区域发展不平衡仍是一个突出矛盾。” 对于我国区域协调发展的总体现状,国家发展和改革委员会副秘书长范恒山对《瞭望》 新闻周刊记者如此概括。

正因如此,按照十九大部署,“以城市群为主体构建大中小城市和小城镇协调发展的城镇格局,加快农业转移人口市民化” 成为了区域协调发展的又一新指向。在业内专家看来,这种城镇新格局为县域经济发展提供了难得的机遇。

县域经济由于自身的辐射面有限,在发展上往往受到诸多制约。一方面,县域财力和辐射力有限,仅凭自身难以形成较大产业集群； 另一方面,推进产业升级或是培育壮大新的产业,县域也缺乏足够的资金、技术、人才、管理等要素支撑。

“构建大中小城市和小城镇协调发展的城镇格局” ,尤需弥补县域因资源匮乏带来的发展短板。现实中,曾经一度落后的农业地区,通过引入战略合作方共同建设智工业园区的探索,为破解县域经济难题找到了切实可行的路径。

采访中,相关专家表示,运用优势资源补齐县域发展短板、探索社会资本参与城镇综合开发新路、以产业集群引领区域转型升级等特质,为 PPP 探索出了一条可持续路径。这一模式的复制与推广,也将助力县域拓展新的发展空间,助力协调发展城镇格局的构建,进而为新时代的高质量发展提供新的动力。

释放区域协调发展新空间

在这一思路指引下,我国新型城镇化快速发展,不仅有力支撑着现代化建设,成为培育发展新动能和推进供给侧结构性改革的重要抓手,而且有效发挥着对区域和农村的辐射带动作用,为缩小城乡发展差距、推进城乡发展一体化作出了重要贡献。

回顾我国的城镇化发展历程,肖金成也对本刊记者表示,随着城镇化的不断推进,我国的城市数量不断增加,城市规模不断扩大,形成了多个城市群。城市群对产业的承载能力不断增强，对人口的吸纳能力不断提高,对区域的辐射带动能力和国际市场竞争力日益扩大。

“未来,应着力促进大中小城市和小城镇协调发展,形成合理的城镇体系,带动更大区域的经济发展。”应以城市群带动和支撑区域发展,促进群区耦合联动； 促进产城融合,推动新型工业化、信息化、城镇化、农业现代化同步发展； 发展特色小镇，促进城乡融合,带动农村地区发展； 促进通过深化户籍制度改革和对进入城市的农业转移人口提供均等化的公共服务,促进农业转移人口市民化。

受访专家表示,在此过程中,促进约 1 亿农业转移人口落户城镇,改造约 1 亿人居住的城镇棚户区和城中村,引导约 1 亿人在中西部地区就近城镇化,解决好这“三个 1 亿人” 问题,关键是要建立多元

化可持续的城镇化投融资机制。

实践中,一些地方正是由于这一机制的缺乏,只能依托于平台公司融资,产生了风险分配不合理、明股实债、政府变相兜底，以及社会资本融资杠杆倍数过高等问题,积累了隐性债务风险。

专家们认为,在企业与地方政府的合作中,华夏幸福创造性地引入了一套互利共赢机制,即除了接受严格的绩效考评、满足物有所值和财承评价等条件之外,企业只有帮助政府实现发展目标和增量财政,才能获取收益,与政府的利益高度一致。有研究人士认为,这一探索在推进经济转型和可持续发展的新型城市建设中都具有示范价值,也有助于拓展区域协调发展新的空间。

PPP 提升区域发展综合价值

一方面要加强城市群建设,同时要强化大城市对中小城市的辐射和带动作用,逐步形成横向错位发展、纵向分工协作的发展格局。完善城市群协调机制,加快城际快速交通体系建设,推动城市间产业分工、基础设施、生态保护、环境治理等协调联动，促进形成大中小城市和小城镇协调发展的城镇格局。

为县域发展注入创新动能

县域发展历来为国家重视。去年 5 月 ,国务院办公厅印发 《关于县域创新驱动发展的若干意见》（以下简称《意见》 ）,部署推动县域创新驱动发展工作。《意见》 指出,新形势下,支持县域开展以科技创新为核心的全面创新,发挥科技创新在县域供给侧结构性改革中的支撑和引领作用,打造发展新引擎,培育发展新动能,实现县域经济社会协调发展,对于建设创新型国家乃至全面建成小康社会意义重大。

在《意见》 部署的县域创新驱动发展八项重点任务中,加快产业转型升级,促进县域特色主导产业向绿色化、品牌化、高端化、集群化发展位列首位。这一指导《意见》 给已经行走在这一轨道上的企业提供了更强劲的动力。

xxx 年是我省公安机关开展 “基层基础建设攻坚战” 的开局之年,由于智工业园区警务的基础性、先导性作用,做实做强智工业园区警务是决胜的前提,因此拟在我区试点 “智工业园区社会综合治理云平台平台”,主要功能是在管理服务对象的移动终端安装 APP,服务管理对象在该 APP 的管理下采集提报信息,开展巡防巡查,与智工业园区民警通过语音文字图像视频进行互动交流， 智工业园区民警利用后台对所管理服务对象提供的信息进行 查看、提报,获取管理服务对象的轨迹点位信息,对管理服务对 象的信息、求助、咨询、报警等纳入公安网相应后台进行流程处 理,从而实现智工业园区社会综合治理云平台。

1.2.项目建设必要性

项目建设必要性

（一） 智工业园区民警的专职化需求

在我区全面实行智工业园区民警专职化,推行“ 1+2+N” 的城区智工业园区警务模式,这里面的“ N”包括警务助理、社会化巡防人员、安保人员、网格员、信息员、特种行业从业人员等，如不采用信息化管理,将导致智工业园区民警无法对人员的轨迹行踪进行管控,不利于建立智工业园区民警工作长效机制。

（二） 智工业园区警务工作复杂性需求

智工业园区工作的巡逻防范,常住人口、暂住人口、重点人口管理,收集情报信息、排查矛盾纠纷,对治安热点进行管理，开展便民服务和接处警等工作,如离开信息化支撑,将是无源之水无本之木,难以维持。

（三） 警种部门支援智工业园区警务工作并获取智工业园区

警务支持的需求

如没有信息化平台,警种部门无法对智工业园区民警进行信息支持,也无法通过智工业园区发送搜集重点。总之,智工业园区社会综合治理云平台工作增强智工业园区警务工作的基础科技支撑力,为智工业园区警务工作提供重要的支持。

1.3.项目建设目标

1、实现基于位置的管理服务对象管理体系。警务助理、信息员、巡防安保人员等安装手机 APP,从而实现与智工业园区民警的互动交流,智工业园区民警对所管理服务对象的位置一目了然,从而实现智工业园区警务工作的信息化。

2、实现信息的社会化源头采集。维稳信息、人员信息等通过社会人员直接从源头采集入库,智工业园区民警得到了进一步解放,也杜绝了“治安云” 中数据造假现象。

3、加强对重点管理单位的安保。通过系统的排班、巡防、执勤等勤务报备,智工业园区民警对重点安防单位安防从业人员的状态一目了然,并能直接发起对讲,加强企业自身安防能力。

4、接处警、防爆反恐等公安工作获得社会力量的支持。平时智工业园区民警对所掌控的安保力量进行一定的培训,在接处警、防爆反恐等工作时可安排社会力量介入,从而进一步提升公安机关打击能力。

1.4.建设原则

（一） 总体规划,分步实施

项目要根据自身实际情况制定分期建设目标和建设内容,分阶段逐步实施。用先进适用的信息技术,有计划、分层次地协调推进,确保本项目建设工作取得成效。

（二） 统一领导,加强协调

由于项目涉及面广、涉及部门多,因此建设实施要在领导小组的统一领导下,按照统一的方案,协同配合,保证项目建设的顺利进行。

（三） 整合资源,注重服务

依托现有的信息化建设成果和成功经验,整合各方的信息资源。通过项目的建设,把分散的、独立的信息资源整合为统一的数据中心，达到互联互通,实现资源共享,真正为领导决策、综合研究、行业运行监管、企业单位和公众提供服务。在保护既往投资的基础上,最大限度地发挥资源整合的放大效应。

（四） 统一标准,保障共享

从洞头智慧城管建设全局出发,统一规划、统一标准,避免出现标准不一的现象。在城市数据中心的数据整合、分类、编码、存储、加工、传输和交换过程中,严格遵循国家有关标准,为今后扩展、升级提供有力保障。

（五） 技术先进,安全可靠

要依靠先进科技技术,借鉴国内外先进经验开展建设工作,注重各系统的可靠性、实用性和先进性,采用符合当前发展趋势的先进技术,并充分考虑技术的成熟性。建立安全防护和容灾备份机制,保障各系统的安全平稳运行。

1、纵向到底、横向到边,打下全业务综合城市管理体系基础

从纵向和横向完善智慧工业园区的运行体制与机制,纵向上完善一级监督（区）、两级指挥（区、街）、三级管理（区、街、社区） 的运行模式,横向上通过实现城市管理各相关业务工作网格的叠加和事部件数据的统一,将城市管理、应急指挥、安全生产、综治维稳等相关业务进行集成,构建以三级联动、多部门协同为特征的全业务综合城市管理体系。

2、升级“数字城管” ,丰富智慧城市基础信息并有效促进信息共享

针对前期“数字城管” 建设有待完善的内容,如监管数据无线采集子系统、业务受理子系统、协调工作子系统、地理编码子系统、监督智慧子系统、综合评价子系统、应用维护子系统、基础数据资源管理子系统、数据交换子系统,通过对原来“数字城管” 系统升级,丰富智慧工业园区的基础资源库。同时,基于“智慧城市” 整体架构，积极推进与其他部门的数据双向共享,提升智慧工业园区的科学性、有效性和及时性,为打破现存的“信息孤岛” 现象做出贡献。

3、完善闭环体系,建立保证城市管理水平持续提升的长效机制

在应用软件方面,通过系统扩展,完善前期“数字城管” 建设缺失的环节； 在监督评价方面,通过建立包含内部和外部评价在内的一整套科学完善的自动监督评价机制,在综合考虑内部管理要求和群众需求的基础上,不断发现城市管理中的盲点和薄弱环节并有针对性地进行整顿和提高,确保城市管理水平的持续提升。

4、积极应用物联感知、数据分析等智慧化技术,为城管业务水平提升提供新助力

城管业务水平的进一步提升,需要得到包括物联网、数据分析等在内的智慧化技术的有力支持。应用物联网技术,在全面采集工况信息的基础上,实现在统一门户管理、城市大数据中心、停车诱导、特种车辆管理、城市照明、智能视频分析、民生服务、煤气网上支付、农村污水管控等领域的智能化管理； 通过引入数据分析技术,辅助用户发现城管问题的发生规律（包括时间维度和空间维度） ,为领导决策提供支持。

5、引入信息采集社会化运营机制,为“服务型政府” 建设做出有益探索

在信息采集环节引入社会力量,不但可以解决机关事业单位人员编制及劳动合同关系问题,而且通过招聘本地人员从事信息采集工作,还可以保证问题发现和处理结果核查的百姓视角,真正做到想百姓之所想、急百姓之所急,为“服务型政府” 建设做出有益探索。

6、建设城市管理可视化应用系统,扩大问题发现来源,提高日常监管工作效率,为用户带来明显的应用价值与管理效益。

1 ） 场景高清化视频监控

在城市广场、公共场所、小摊小贩易聚集场所、菜场、建筑工地、河道沿线等区域部署高清网络球机或全景摄像机,实现对城市各类部件和事件的全方位、全时段的可视化监控管理。

2） 事件可视化联动管理

根据城管综合执法、市政、环卫、渣土各业务部门的管理需要采用视频智能分析技术实现智能监测和联动告警策略,包括对于人行道内的违法停车、出店经营、乱堆乱放等固定场景的违法行为进行管理，

做到自动辨别并将提示报警,相关信息进行人工辅助分析,清晰地记录违章行为照片和违章过程录像。

3） 调度可视化决策分析

未来通过城市视频监控系统的联网,实现各相关专业部门 --- 区级--- 市级的多级城管视频监控联网应用。包括整合公安交警、交通、工商、环保等其他部门已建视频监控资源,实现资源的有效共享并实现城管部门对城市突发应急事件的可视化指挥调度和参考决策分析。

第二章 园区创新发展趋势

2.1 园区经济向生态型转变

经过多年的发展,园区积累了丰富的产业,形成了企业聚集发展的态势,但是,我国的园区在开发建设的快速推进过程中，仅仅解决了产业“进区入园”,即只关注了产业的地理集中或产业集聚问题,而没有解决产业的 式发展和集群化竞争。随着国家优 政策统一化、土地、环保政策趋 ,单 依靠规模效益的放型园区经济发展方式已经难以为 。

在可持续发展的压力下,园区迫切需要改变园区内产业间、产业内部关联度低、配套性差、资源利用

率低的状况，着力完善产业 和产业配套，促进资源利用由“资源 - 产品 - 废物” 的现行模式向“资源 - 产品 - 废物 - 再生资源” 的循环模式转变，尽量减少生产端的资源投入、尽可能延长产品的使用周期与效率、最大限度地减少废弃物，实现资源再循环。显然，在两型社会的要求下，建设“资源循环、经济发展” 的生态型园区，促进产业的生态化和生产、生活、生态的协调发展，是今后我国各类园区发展的大趋势。

2.2 园区企业向高新型转变

在激烈的园区竞争背景下，园区的产业同质化竞争也日趋严重。从世界范围来看，产业 的附加值主要向产业 的两端延伸，在研发、设计、创新等上游领域和现代物流、展销服务等下游领域存在着较为丰厚的利润空间，而我国多数园区的产业体系都处于产业 的中间环节。

在竞争的压力下，为了抢占产业 的高附加值端，园区内的企业日益增加研发投入，转变以往单 生产制造的发展方式，向高新型企业演进，通过不断的技术创新保持竞争领先优势。显然，在园区“二次创业”的过程中，推动园区企业向高新型转变，扶持具有发展潜力的创新型中小企业，尽快占据科技制高点，促使园区从“制造” 转向“创造” 转变，是我国园区企业发展的趋势。

2.3 园区管理向城市化转变

高水平的产业需要高水平的人才聚集。随着园区的不断发展，园区内的人员日益增多，社会功能需求日益复杂，需要有与之相配套的生产生活环境，单 以工厂为主导的园区很难成就高水平的产业集群。之前我国园区以发展经济为主，社会服务职能相对缺失，随着经济社会的发展，园区必须摈弃单 工业化的发展思路，转以城市开发的角度去看待园区。

在新的形势下，被征地农民的安置、社区建设与管理、环境保护、教育卫生、社会保障等社会服务职能的拓展与完善成为园区未来在管理体制创新中的重要方向，管理机构必须将园区的发展纳入到城市/区域的整体空间规划中，承接更多城市功能的转移，并拓展新产生的城市职能。因此，在和谐社会的要求下，园 区管理机构将更加注重满足社会功能需求，园区管理方式也将向城市化转变。

第三章 工业园区大数据存在的问题

信息化是全球经济和社会发展的大趋势，也是园区提升产业效能和率先实现现代化的关键环节。但是，在多年的园区发展中，信息化建设长期处于被忽视的地位，信息化水平与园区社会经济发展水平并不一致，与园区的发展要求与定位也不相适应。

3.1 信息化配套设施及服务不够完善

园区配套设施建设一直聚焦于交通运输、供水、供电、排污等市政基础设施，近年来信息基础设施的建设正逐渐受到园区管理机构、入驻企业的重视，但由于工业园区大数据建设起步晚、时间短，信息化配

套设施及服务还不够完善。

首先体现在信息基础设施建设落后。据赛迪信息调研发现，园区多处于城市边缘位置,移动通信服务没有伴随园区的扩张而覆盖新开发区域,或多或少的存在着移动通讯覆盖面窄、信号不稳定等问题。在通信网络建设方面,存在着网络承载能力低,互联网总体接入带宽偏小的问题,光纤入户比例低,无法充分满足企业及居民生产生活的需求。在无线接入建设方面,无线接入点少,覆盖面窄,而且接入带宽小,大多局限于政府、企业办公区域,没有与移动通信网络及与固定通信网络一起形成全覆盖、无间隙的信息网络。

其次,信息化配套设施、服务效能偏低。园区基本建立了数据中心为企业提供主机托管、互联网接入等服务,但还没有建立共享共用的容灾备份中心,呼叫中心,将各种计算能力、存储能力整合并虚拟化,进而提供高效、集约的云服务的情况就更少了。已有的数据中心的作用没有完全发挥,在增值服务方面还存在着较大的发展空间和潜力。信息化公共服务平台建设是解决中小企业信息化难题的重要手段,目前的信息化公共服务平台还存在着服务种类少,使用效率低的情况。

3.2 信息资源整合利用工作严重滞后

目前各类园区和园区内各个部门都在积极开展信息化建设，信息化工作也有了一定的基础。但由于缺乏统一的规划和指导，各个部门过分强调自身的特殊性,条块分割现象严重,突出表现为一些纵向信息网络自成体系,业务系统封闭运行,不能实现互联互通等,形成了许许多多“信息孤岛”,难以实现信息资源共享。特别是在一些“金” 字工程单位,上、下信息交流畅通,但与其他委、办、局之间的横向信息交流共享困难。

由于信息孤岛的存在,许多园区更加忽视了信息资源的开发利用,集中表现为数据资源较为分散,信息集成共享度不高。虽然园区网络和业务系统发展速度很快,但信息资源的开发利用却没有提到应有高度,缺少园区信息资源交换平台与中心,普遍存在信息资源规模小、范围窄、质量差、更新周期长、共享程度低等问题。目前,绝大多数园区的信息资源,尤其是大型的公共数据库和主题专用数据库开发滞后,社会可利用的信息资源更加不足； 商业性的信息资源开发工作尚未起步； 另一方面,公共基础数据采集、共享、交换、维护、储存、利用和发布的规范和标准尚未建立,信息资源的开发和利用缺乏有效的激励机制。

3.3 智慧化推进工作缺乏有效抓手

作为新型工业化的核心内容。智慧化是信息化和工业化的高层次的深度结合,是指以信息化带动工业化、以工业化促进信息化,走新型工业化道路,智慧化的核心就是信息化支撑,追求可持续发展模式。也成为了园区新型工业化发展的重要动力。智慧化的主体是企业,企业既是经济发展的主体,也是信息化建设的主体,必然成为“智慧” 融合的主体,推进“智慧” 融合最终也要落在企业身上。在园区推进智慧化的过程中,一方面以重大项目作为智慧化的切入点,这打开了园区智慧化的工作局面。另一方面建立公共技术服务平台,为中小企业提供更多的技术支持。

但是,园区在推进智慧化的过程中,大型智慧化项目使得园区大型、骨干企业得到了更多的扶持,而众多的中小企业得到了更少的资源； 而公共技术服务平台虽然投入运行,但是发挥作用有限,很多企业仍然不重视信息化工作,信息化建设力度不大，而有些企业在信息化投入的积极性高与时效性低之间的矛盾也

非常突出,还存在信息化投入的盲目性,未能形成有利的企业信息化氛围。同时,企业信息化专业人才普遍缺乏,人才引入、使用机制不健全、不完善,信息化培训教育工作滞后等问题是亟待解决的问题,信息化专业人才匮乏已成为制约企业信息化建设的重要原因。

3.4 园区综合管理缺乏智能化手段

目前园区城市综合管理的内容主要局限在城市事件的管理上,对于城市的组成部件、运行状态的信息采集、管理功能偏少，仅有的部件管理也集中在地上设施,而供气、供水、供热、弱电管网等地下基础设施的信息采集功能匮乏。同时城市事件的管理范围仅仅局限在城市交通、治安监控等几个方面,而没有覆盖到城市经济管理、空间管理、住宅管理、建筑管理等领域。

造成以上状况的原因是因为目前园区城市综合管理缺乏智能化手段,以人工巡查为主,部件、事件发生变化无法实现与城市管理机构的及时自动通信,城市管理缺乏智能性、主动性,城市综合管理中的问题上传、处理分配、结果反馈等各个环节都缺乏自动化处理手段,同时城市综合管理的应急预案的数字化程度较低,应急预案启动后仍然依靠人工按照流程进行通知,无法第一时间知会各个相关部门,造成应急反应时间延长。城市管理智能化技术及智能化手段的缺乏,使得城市设施静态管理、动态运行监控、智能化运行维护、自动应急指挥处置等全方位城市综合管理能力严重低下。

3.5 节能环保新技术应用匮乏

在节能减排方面,用信息技术改造传统行业,尤其是改造重点用能行业的广度和深度不高。对于园区多数型企业,信息技术主要被应用于管理环节,例如集中建设的 OA、ERP 等信息系统,而利用信息技术对生产全程实现数字化监控,将物联网、移动互联网等新一代信息技术,渗透到工具、工艺、流程中,实现对生产管理全流程的“泛在感知”,最大限度地降低各种资源消耗的例子明显偏少； 比如利用物联网技术,实现路灯根据天气状况自动开启关闭的技术已经成熟,但是应用少见。新技术应用在促进节能减排方面的巨大潜力还没有得到充分发挥。

第四章 智慧工业园区大数据建设目的

4.1 智慧化提升园区吸引力

随着园区经济的高速发展和经济全球化带来的机遇,国内各类成熟园区已经开始转型升级,新兴园区正借助后发优势力争实现弯道超车,所带来的结果就是园区招商与服务对象已经从劳动密集型企业迅速转向技术密集型企业。技术密集型企业因为技术含量高、更注重绿色环保、雇佣人员素质较高,所以可以为园区以及地方政府带来更加优质的经济和社会效益,但在同时,也对园区管理提出了更高的服务需求。

智慧园区建设,一方面可以提升园区内部的政务管理能力，增强园区在推动企业创新上的服务能力； 另一方面通过智慧园区建设,促进节能环保,可以改善园区居民生活环境,显著提升生活质量；

更重要的是为园区内的企业服务,通过智慧的基础设施、智慧的政府服务、智慧的公共服务体系,为企业提供优良的创新、发展环境,消除企业发展的后顾之忧,并适时的为企业发展提供各种支持。通过智慧园区的建设,把园区管理机构、园区企业、园区居民等园区内各方的优势资源加以整合并通过各种途径大力推广,为园区打造一个整体的优质品牌,可以显著提升园区对优质企业、高素质人才的吸引力和凝聚力。

4.2 智慧化促进园区可持续发展

经过多年的开发与积累,我国园区正处在工业化、城镇化快速发展时期。***8 年以来国家实行了一系列措施,统一了内外资税率、明确了基准地价,规范了地方政策,这使得园区的政策、成本优势被严重削弱,同时国家严厉的土地、环境政策使得园区空间拓展、经济发展受到一定的限制,依靠规模效益的 放型园区经济发展方式已经难以为 ,可持续发展的压力持续增大。

而信息化在有效降低资源、能源消耗,减轻人员负担等方面,具有传统手段无可比拟的优越性。通过信息技术创造先进的智能工具,改造提升传统产业,提高物质能量开发利用水平,开发新资源,改善产业结构,提高社会效率,降低环境污染,实现节能减排、发展绿色经济,使许多悲观难题迎刃而解,因此信息化是实现园区可持续发展的必由之路和高级阶段,而且可持续发展需求为智慧园区建设提供了广阔的发展空间。因此,在新形势下园区迫切需要通过以信息化为核心的智慧园区建设来破解难题实现可持续发展。

4.3 智慧化助力园区发展战略性新兴产业

战略性新兴产业是引导未来经济社会发展的重要力量,发展战略性新兴产业已成为世界主要国家抢占新一轮经济和科技发展制高点的重大战略。“十二五” 时期,各类园区之间对于战略性新兴产业发展的资源要素和产业间的竞争不断升级。

战略性新兴产业是以重大技术突破和重大发展需求为基础,知识技术密集,以创新为主要驱动力的产业。园区要在争夺战略性新兴产业资金、项目、企业的竞争中脱颖而出,需要将信息技术渗透到园区生产、经营、管理、生活的各个方面,围绕“管理” 、“引导” 和“服务” 三大工作核心,以信息技术的创新应用最大程度地整合各种创新资源及生产要素,实现创新资源和创新主体的有效聚集和有效流动,营造园区创新环境,加速创新进程,帮助园区实现 “关键产业培育壮大”、“创造现代智能园区环境” 、“提供高效便捷公共服务” 三大任务,扩大园区影响力、抢占战略性新兴产业发展的先机。

4.4 智慧化顺应信息技术创新与应用趋势

目前世界范围内的电子信息技术的发展日新月异,信息技术的创新不断催生出新技术、新产品和新应用,信息技术革命所带来的影响由单 科学技术领域向生产、管理、生活领域全面渗透。

信息技术的突破发展,使得之前因体制、技术原因而不能实现的资源共享、政务协同等变成技术可行,同时信息化认识水平的提升要求园区管理机构采用信息技术提供更加方便快捷的公共服务,提供了破解“条块结合” 难题、创新园区管理体制的契机。同时信息技术的飞速发展,要求智慧园区的基础设施、业务系统的建设必须准确把握信息技术的发展趋势,充分考虑信息技术创新带来影响,既要避免系统建成就过时导致的资源浪费,也要避免超前建设造成的资源浪费。因此智慧园区建设过程中应合理采用先进、成熟的信息技术及管理模式,有所为有所不为,尽量避免或减轻信息技术革命对智慧园区建设进程造成的冲击。

第五章 智慧园区总体构架

当前园区的主要工作是如何在资源 缺的背景下,创造更多的价值,实现园区经济转型、社会和谐。利用电子信息技术的深度应用与融合,提升园区政府的管理、服务、引导能力,提升企业的研发设计、生产制造、经营管理的效率,提升园区运行的智能、顺畅程度,提升园区居民生活的便利水平,是智慧园区建设的主要任务。

智慧园区由基础设施、信息资源、业务应用、运行保障四个层次组成

5.1 新一代信息基础设施

通过构建新一代信息基础设施,为园区内的组织和个人提供安全、高速、便捷的网络环境,实现园区内的部件、人员随时随地接入网络,奠定了泛在感知的网络基础。新一代的信息基础设主要包括两个层面,全面覆盖的感知层和泛在的传输网络层。

全面覆盖的感知层由各种传感器以及传感器网关构成,不同区域、不同行业采用的感知方式也不尽相同。通过信号、ID 和位置感知网络的全面建设,实现对园区主要的公共场所、野外水源、家庭住宅、生产场地和移动车辆等实现感知网络的全面覆盖，使得园区各元素的各类信息均可接入到传输网络层。

泛在的传输网络层建设以泛在接入、高速传输、安全融合为目 的,高标准、高起点、集约化规划和建设面向未来的 FTTx 网络,大规模部署高速无线宽带覆盖,促进电信网、互联网、广电网的融合,构建大宽带、全业务融合的有线无线高速的全覆盖网络,实现多种方式随时随地接入。

5.2 集约共享的信息资源利用体系

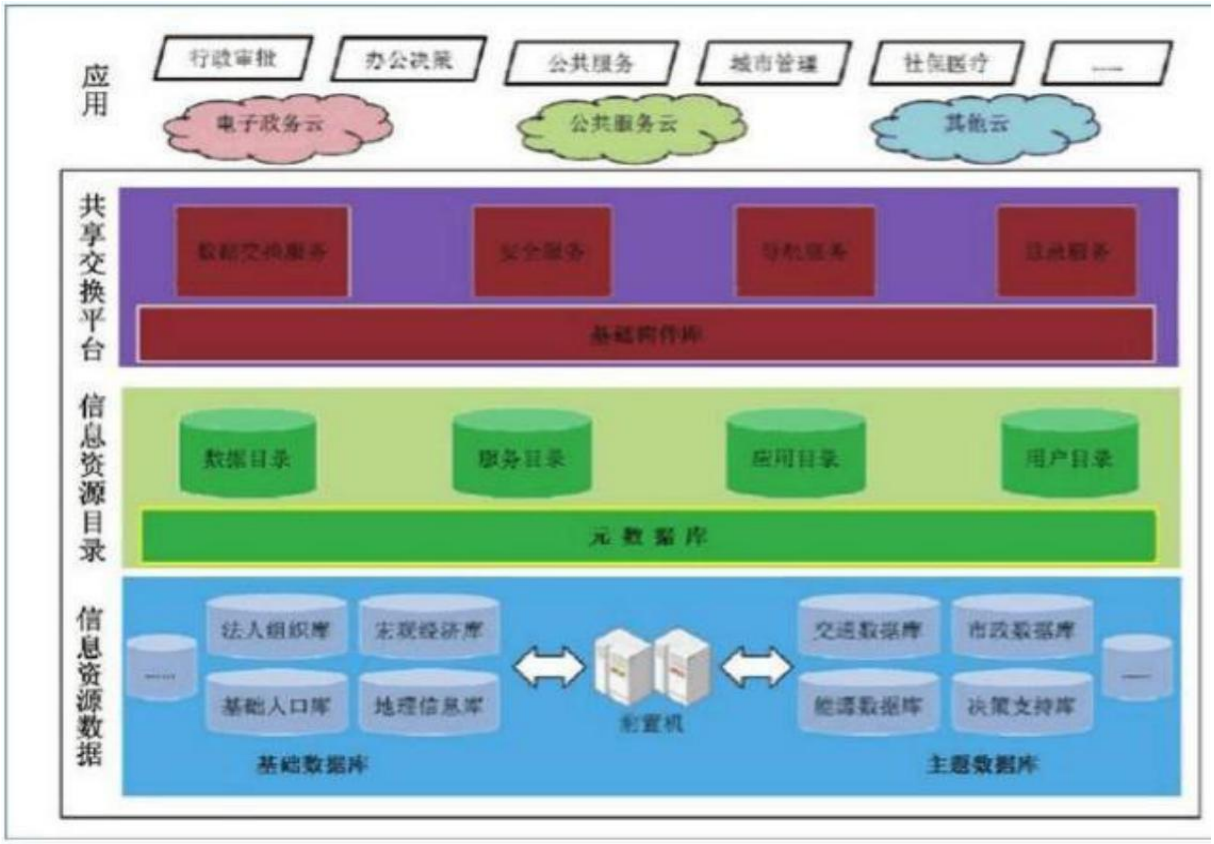
信息资源建设体系应在园区已有的政务信息化基础上,遵循国家电子政务总体框架和国家有关标准要求,在智慧园区建设的统筹规划下,依照“一体化” 集约共享的建设思路,以服务为宗旨,以应用为关键,以信息资源开发利用为主线,通过安全、通畅的信息资源交换,实现园区各单位间资源共享,达到业务协同。

集约共享的信息资源体系主要包括三个层次:

信息资源数据主要包括两种,一种是四大基础数据库,其次是园区管理、服务所需要的各类主题数据库,例如市政数据库、决策支持数据库等,信息资源数据还包括视频监控、传感器、RFID 等感知层上传的数据。

信息资源目录体系的建设应遵循国家电子政务信息资源交换体系标准,规划和完善园区内各类主题的应用框架,建立跨部门、跨行业交换和共享的业务资源指标体系,实现不同部门、不同行业间的资源共享。

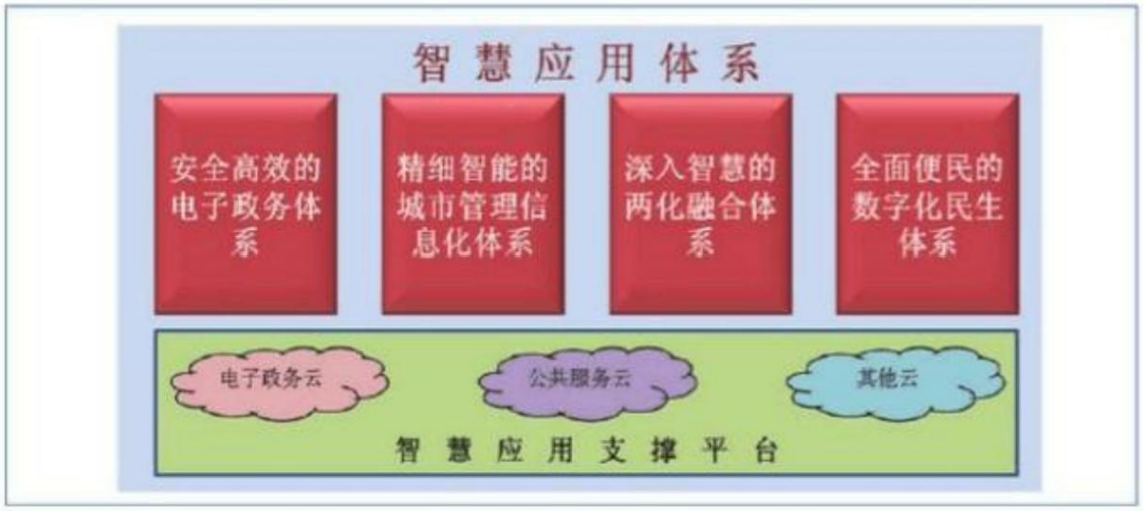
共享交换平台是业务系统间无缝共享数据、连通信息孤岛的高速公路,为实现应用层各种应用系统的搭建和运行提供支撑服务，包括目录服务系统、交换服务系统、安全服务系统和导航服 务、平台管理服务等。



集约共享的信息资源利用体系打破了信息孤岛,实现数据共享从部门级到区域级的提升。通过加强数据的统一管理,可以保证数据的准确性和及时性； 通过数据的共享交换,实现了智慧园区运营的高效协同,实现了由数据转化为价值。

5.3 智慧应用体系

智慧应用体系是智慧园区建设重要的部分,也是可以直接提升园区管理服务能力、生产生活环境的重要构成,智慧应用体系分析、整合园区运行核心系统的各项关键信息,从而对于包括民生、环保、公共安全、城市服务、工商业活动在内的各种需求做出智能响应,使园区运行更加智慧顺畅,为人类创造更美好的城市生活。智慧应用体系包括一个支撑平台和四个应用体系。



智慧应用支撑平台是基于云计算技术,通过网络把多个成本相对较低的计算实体整合成一个具有强大计算、存储能力的完美系统,并借助 SaaS、PaaS、IaaS 等模式把这强大的计算、存储能力分配到终端用户手中。“云” 中的资源在使用者看来是可以无限扩展的,并且可以随时获取,按需使用。

安全高效的的电子政务体系以网络为依托,以社会的需求为中心,以“政府就是服务” 为出发点,以先进的信息技术为手段，将传统的政府管理、服务工作移植到网络化、数字化的环境中，帮助企业、公众、社会组织等快速、高效地解决各种事务,协调各种关系。电子政务体系包括网上协同办公、联合行政审批、行政监察、经济运行调节、市场监管、招商引资管理等多种政府管理、服务功能,实现政府管理与服务从“一个政府、多个部门”向“多个部门、一个政府” 模式转变。

精细智能的城市管理信息化体系以构建更为高效有序的城市管理模式为目标,依托物联网、云计算等应用理念及最新的电子信息技术成果,广泛布局立体感知、可靠传输、智能处理的感知网络,特别是探索在尽可能多的城市基础设施（如道路、交通信号灯、电灯杆等） 上,附载以 RFID 技术、无线传感网络技术等为核心的新型感知终端,全面、实时、准确获取城市运行的相关信息,在园区安全、交通管理、环境保护、应急指挥、能源管理等方面实现城市运营管理从“平面管理” 向“立体管理” 的转变,提高城市运营管理的精细化、智能化水平。

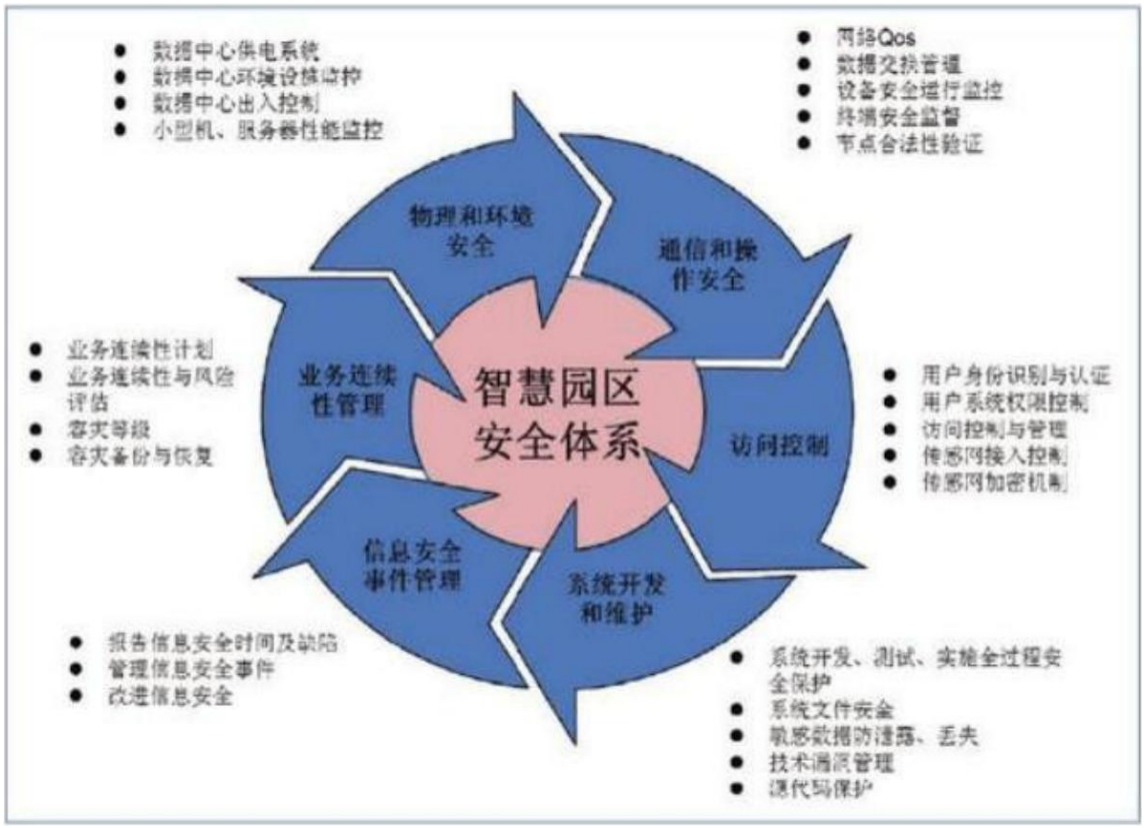
深入智慧的智慧化体系是园区推动经济转型走新型工业化道路的重要抓手,智慧化体系包括提升传统产业智慧化水平、扶持壮大新型融合智慧产业、建立扶持有利的公共服务体系等。通过深入智慧的智慧化体系提升园区内企业对信息化技术手段和管理工具的应用意识,加强对各类嵌入式的信息产品以及计算机辅助设计/制造/工程/工艺等技术、自动控制技术、ERP 等业务系统的应用,促进信息技术与生产技术、产品、业务、产业的全 方位融合,提升园区产业创新能力与发展水平,促进

产业结构优化升级,加快经济发展方式转变。

全面便民的数字化民生体系应当坚持以人为本、城乡一体、服务为先,重点加强教育、文化、卫生和社区等领域信息化建设，形成新型的全方位的信息化公共服务应用体系,推动电子政务、公共服务事业、电子商务向社区、街道延伸,不断提高服务质量，丰富服务内容,努力实现公共服务的普遍、优质和高效,为园区群众构建亲民、便民的数字化生活环境。

5.4 智慧园区安全体系

智慧园区安全体系需准确建立在业务流程整合、业务数据规范交互基础之上,从信息系统等级保护角度提出安全体系的设计思路和安全防护策略,以“整体合规、资源可控、数据可信、持续发展”的生存管理与安全运维模式,详细分析智慧园区安全体系建设的必要性,界定智慧园区网络区域边界范围、安全保障技术路线、安全防护策略等,以此为园区服务机构、管理机构及社会公众等提供安全有效、规范合规的信息服务。



智慧园区安全体系包括安全的信息感知、可靠的数据传送和安全的信息操控三方面,具体涉及物理环境安全、通信管理、访问控制、系统开发和维护、信息安全事件管理、业务连续性管理六个层面,并且在每个层面上,都包含安全管理和安全策略的内容。

5.5 智慧园区管理体系

智慧园区管理体系是对智慧园区规划及建设中所涉及的组织机构、制度规范、IT 资产（智慧园

区建设涉及的硬件系统、软件系统、IT 业务流程,以及建立在这些系统和流程之上的、建设单位内部业务流程与知识资源的总和)、安全、运行维护资金等进行管理,有效的融合组织、制度、流程和技术,制定和完善相应的管理制度,实施规范和专业化管理,落实运行维护费用,使智慧园区管理体系成为智慧园区建设的重要组成部分,并通过持续改进管理工作,完善 IT 管理过程中各个流程管理来确保智慧园区健康运行,达到建设的预期目标。

智慧园区组织建设要求确定和规范智慧园区管理体系的管理方式和与之相配套的人员岗位职责安排、机构设置,将智慧园区管理体系相关的全部活动进行统一决策与规划,形成集中统一的智慧园区管理机制。

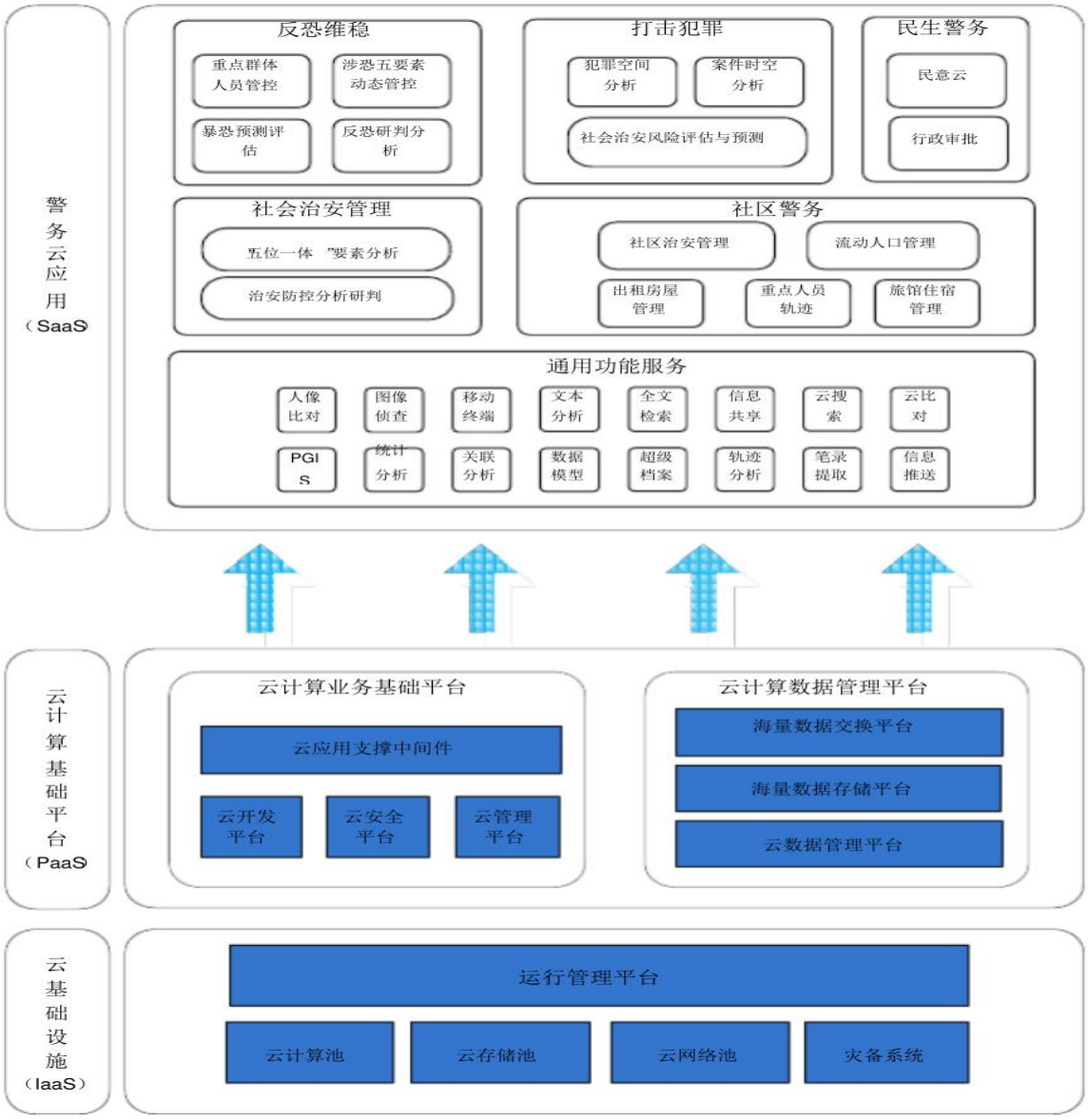
智慧园区制度规范建设分别从管理与操作方面建立智慧园区建设管理过程中各个参与要素(人、流程、工具) 的行为准则与工作程序,从智慧园区管理体系总体运行、流程执行和岗位职责三个层次建立考核评价体系,确定智慧园区建设费用的组成与计算方式,规范智慧园区建设费用的来源保障,实现智慧园区建设管理的量化管理。

第六章 系统核心组件

6.1 系统总体设计

系统总体架构共分为网络通讯层、硬件层、数据层、支撑层、应用层几个模块组成。

图1. 平台总体设计图



网络通讯层

利用运营商 3G、4G 移动网络以及宽带有线网络,配合公安边界平台整合的公安内、外网,构建智工业园区社会综合治理云平台基层基础工作平台,为信息数据传输提供安全、顺畅的交换通道。

硬件层

利用服务器、交换机、存储设备、防火墙等硬件设备,为数据的存储、交换、共享、分析、处理等提供基础硬件介质。

数据层

通过对智工业园区治安防控基础数据库、地理空间数据库、决策支持引擎库、日志库及数据访问、共享接口等业务进行分析和调用,建立系统所需的数据池,便于上层应用的分析和调取。支撑层

根据业务需求对数据进行处理,通过开发消息服务、定位服务、通讯服务、应用服务,实现互联网应用端、互联网服务端、公安网服务端、公安网应用端的数据交互与应用。

应用层

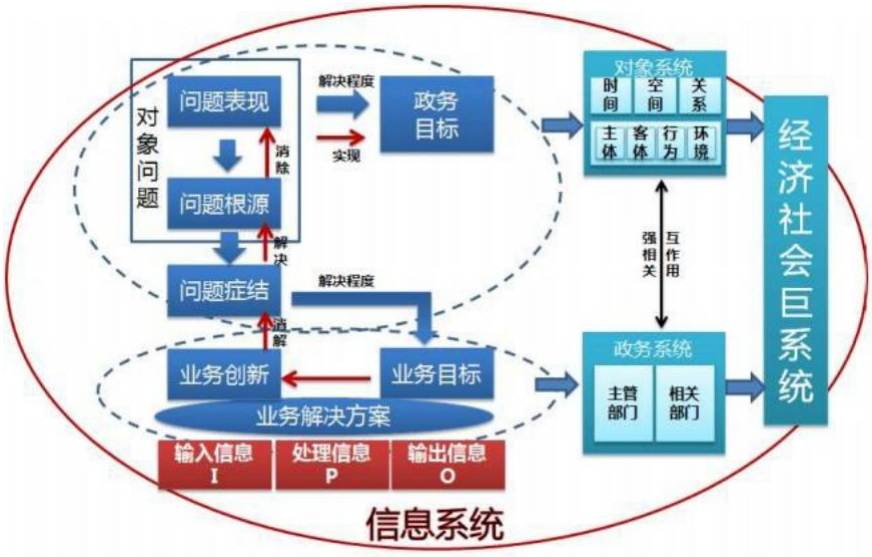
通过智工业园区警务资源图上展现、智工业园区治安防控情报信息上报、一键报警、警务即时

通信、巡防报备、勤务监督等功能模块,实现“信息上报一体化、群防群治一体化、指挥调度一体化、绩效统计一体化” 的智慧智工业园区警务格局。

6.2 系统网络架构设计

根据智工业园区社会综合治理云平台应用人群和业务特点，系统核心服务器部署在互联网,系统基于运营商移动 3G/4G 网络,社会面警务助理、智工业园区民警采用统一配备的智能终端（手机），智工业园区民警办公场所配备互联网接入线路,通过值班电脑对智工业园区警务统一信息接收和指挥管理。

与公安信息专网建立数据交互服务,网络通过公安安全边界实现与公安信息网、视频专网等多网数据的融合网络架构。报警信息数据进入报警平台； 咨询、投诉、举报信息数据进入民生警务平台；民众报送的信息进入“治安云平台” 。



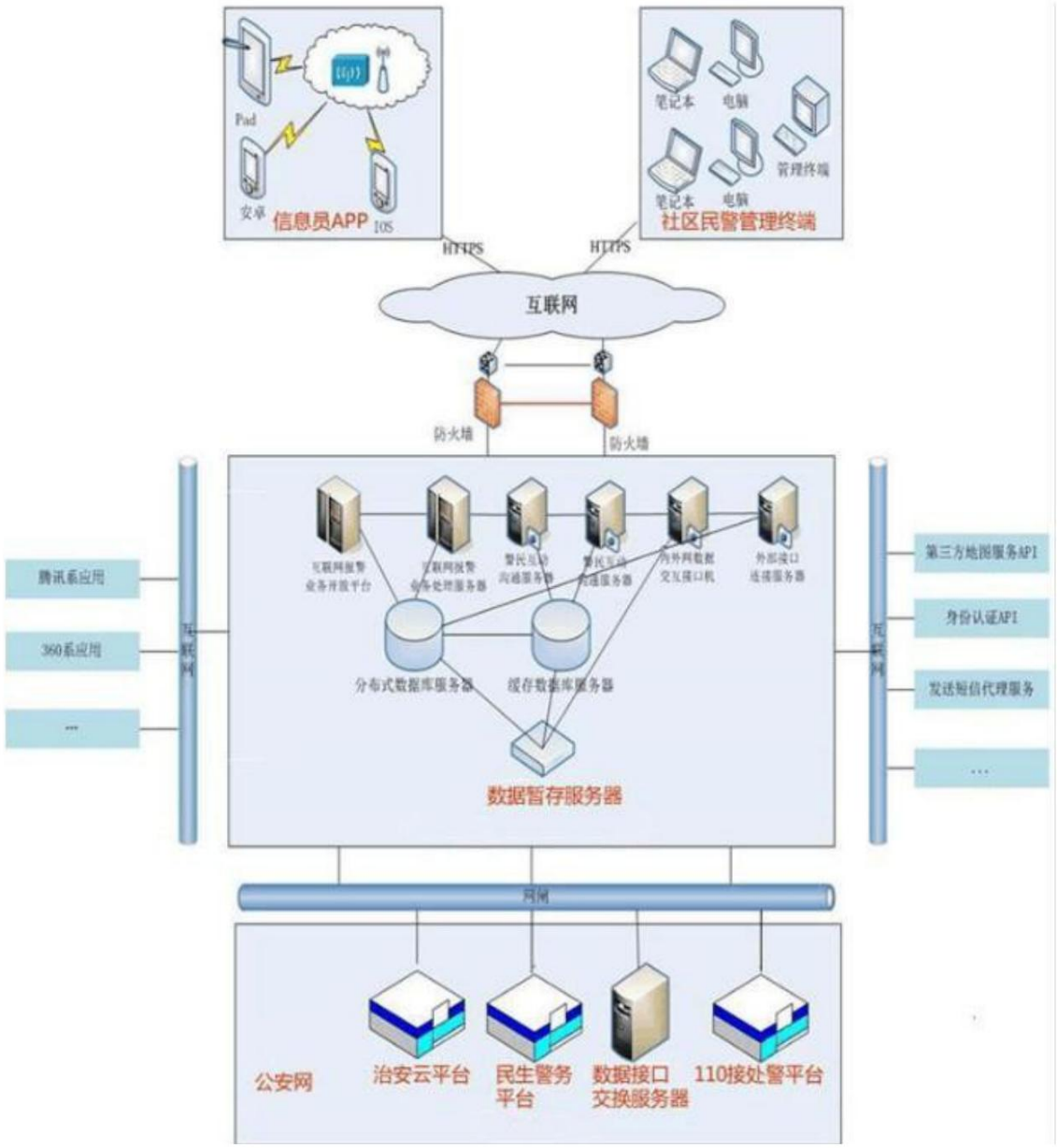


图2.　平台网络架构设计图

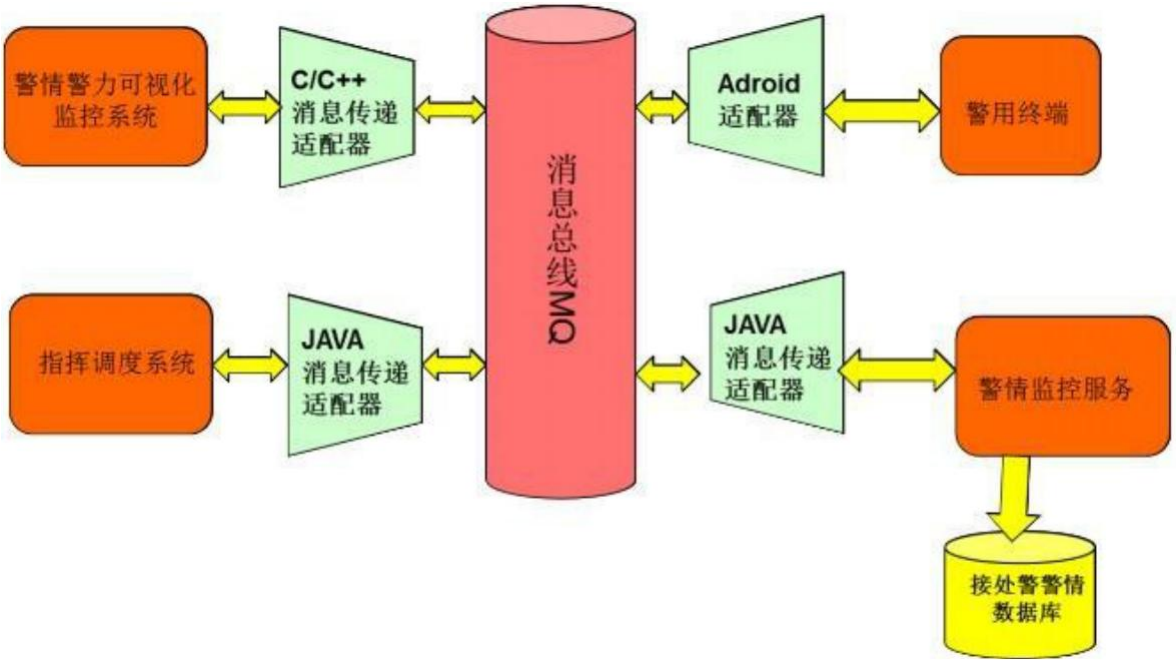
6.3 底层消息交互组件

底层消息交互组件实现系统各个组件之间消息的推送； 包括移动终端与后台系统之间的消息推送, 以及后台系统与外部资源对接的核心承载服务。

6.3.1 消息服务机制

采用消息推送机制, 实现海量信息的队列推送。这是一种推送消息的队列服务器, 即一种消息推送的媒介。它给应用程序提供了一个信息发送和接收的公共平台, 消息被接收之前都可安全保存。

本平台中,移动终端与后台系统实现无线网络通讯,网络信号可能出现抖动,消息推送机制能够支持断点推送,网络信号差时， 消息保持在队列中,当网络信号正常后,消息立即推送到移动终端。



6.3.2MQ 的主要特点

可靠性：MQ 在交替操作下仍能保持可靠性,这种可靠性包括持久化、送达确认、发布者确认和高可用性。

灵活的路由：消息到达队列之前通过消息交换机路由。MQ 针对典型路由逻辑设了几种内置的消息交换机类型。想实现更复杂的路由,还可以把消息交换机绑定在一起,或编写自己的消息交换类型作为插件。

集群：本地网络的几个 MQ 服务器可以集群形成单一的逻辑消息队列服务器。

提供联合模型：有的服务器需要比集群更松散和不可靠的关联,MQ 可以为这些服务器提供联合模型。

高可用性的队列 :队列可以跨一个集群的几台机器被映像，即使硬件出现故障仍能保证消息安全。

多协议：MQ 支持多种消息传送协议。

多客户端：MQ 的客户端包含几乎所有能想到的语言版本。

管理的用户界面：MQ 带有易用的管理用户界面,可以从各个方面监控消息队列服务器。

追踪：如果消息系统异常,MQ 可提供追踪支持,找到异常的出处。

插件系统：MQ 带有多种插件,可以不同的方式扩展 MQ,也可以自己编写插件。

6.4 多媒体融合通信服

智慧工业园区民警与管理服务对象之间（警务助理、信息员、巡防安保人员） 通过语音文字图像视频进行互动交流,可为日常巡防、信息上报、协助打击违法犯罪这些工作过程中提供强大的通信支撑,具有集群对讲、音视频通话、地图定位、图像拍传、视频监控、短消息、位置上报、一键告警等多种必备功能,可基于用户性质、单位群组和工作权限进行管理。社群警务移动 APP 基于运营商 3G/4G 网络,覆盖范围广抗干扰能力强,建立对讲时延小,呼通率高,通信稳定可靠可为民警、群众提供低成本、高效率、专业级的通信手段与指挥管控能力。

通过专用网关及接口实现用户现有各种视频系统 （视频监控、视频会议、无线图传、智能手机等） 的统一接入,实现所有视频系统的集中管理与调度,并通过多媒体通信调度服务器实现各种视频系统之间的无缝交互。

6.5 电子地图服务

6.5.1 基础图层数据服务

实现基础图层数据服务,平台通过 GIS 接口对接,实现与GIS 地图数据的接入,地理属性信息浏览、查询、采集。对接以后，针对底图服务基础上,实现以下信息的获取。

点图层信息

包括医院,药店,商场,超市,酒店,银行,电信营业厅、小区,停车场,汽车服务,美容美发、收费站,加油站,火车站， 公交车站、政府机构,科研教育,大厦,宗教场所等信息。

线图层信息

包括市区主干道,省道,国道,县道,高速公路,铁路,其他道路等信息。

面图层信息

包括水库,绿地,绿地公园,湖泊,河流,行政区界（含县界,区界,市界） ,居民地、辖区（分局,派出所,警务室） 等信息。

警用业务图层信息

包括视频监控点、治安卡口点、电子围栏监控点、重点小区、重点单位、重点场所、警情分布等警用业务图层信息。

6.5.2 地图空间图层数据查询服务

实现对地图空间数据进行查询,支持圈选、周边、多边形等方式查询,可设置查询范围,查询类型,视频、学校、医院、服务场所、政府机关、企事业单位、娱乐场所等图层数据的查询。

6.5.3 实现地图上应用基本功能

地图上应用基本功能,主要包括：地图全图显示、放大缩小、鹰眼、撒点、聚合、定位、地图漫游、测距、测面积、清除等功能。

1 ． 全图显示：在屏幕范围内,以全景方式显示整幅地图；

2. 地图缩放：以一定显示比例放大、缩小地图；

3. 地图漫游：在屏幕上移动地图显示范围；

4. 撒点：在地图上撒点显示,可针对事件、警力、视频展现；

5. 聚合：根据地图级别控制资源显示,通过聚合技术实现多点位数据叠加聚合显示,并计算叠加数量。

6. 定位居中：对应资源双击鼠标进行定位居中显示位置；

7. 测距：可以在地图上通过画线操作测量实际距离；

8. 测面积：面积测量功能：可在地图上测量区域面积；

9. 清除：可清除地图上的事故点、事故路段等颜色标记。

6.6 运行维护管理

运行维护管理模块主要包括：组织机构管理、系统用户管理、用户角色管理、用户功能权限管理、系统日志管理等功能。

6.6.1 组织机构管理

组织机构管理按照组织机构代码对应组织机构名称、地图的管理区域的管理预设置,实现对组织机构新增、组织机构删除、组织机构排序、组织机构查询、机构分配岗位、机构分配角色功能。

6.6.2 系统用户管理

用户通过单一的用户访问界面访问系统,这也是用户访问该系统的唯一入口。用户只能在其中进行系统功能的使用。单一的访问方式,一旦用户登录成功,就可以访问到所有的授权服务，并且进行他们的业务信息的检索和浏览。系统可以灵活的添加或删除角色,并赋予新的角色相应的权限功能。

6.6.3 系统权限管理

平台提供了各种功能，不同用户登录到门户系统可访问或调用的功能和服务有所不同，即对各功能模块进行权限控制，定义一个用户能够访问和操作哪些功能模块。

功能权限管理模块可以定义应用系统的功能项列表，将系统中的特定功能项赋予用户或角色，控制用户对于应用系统中各功能项的访问权限。

6.6.4 系统角色管理

角色管理主要是设置用户访问操作的共性角色，如系统管理员、数据管理员、普通用户。根据部门和个人的职能，增加、删除、修改系统角色，可以赋予角色不同的数据、服务、功能访问权限，实现基于角色的访问权限控制策略。可以为用户指定一个或多个角色，并实现用户角色的转换、修改和去除。

6.6.5 系统日志管理

日志管理模块可实现系统日志记录和管理功能。系统日志主要记录各类用户在登录系统后所进行的操作、访问等信息，以及系统调用服务接口的日志信息。可以根据用户名称、访问系统等过滤条件查询日志信息，并根据日志结果审计用户的访问行为，支持对系统日志的删除、备份和恢复的操作。

6.7 系统用户管理

支持系统海量移动终端间的即时消息传送，包括动态创建群组，动态增加、删除群组成员，支持文字、语音、图片、视频等消息格式。

6.8 智工业园区社会综合治理云平台综合态势展示

智工业园区社会综合治理云平台综合态势展示门户，是系统内涵盖的各类警力（社会辅警、警务助理） 资源、社会治安防控情报信息资源、智工业园区群防群治勤务运行信息，以及各类技防资源的汇总展示，以及相应的宏观研判分析结果展示。各级相关领导可借此门户，掌握全区的智工业园区治安防控网络建设情况、群防群治工作的开展情况，以地图、数据、图表、位置、视频等实时态势信息实时展现，从而有效直观了解智工业园区治安防控管理工作。

同时，通过此宏观展现视图，可以快捷的进入相应的应用系统或功能，从而进一步了解细节情况。

主要包含以下几个部分的内容：

6.8.1 智工业园区治安防控情报信息上报汇总

系统通过柱状图形式动态展现当日接报的智工业园区治安防控社群主动上报信息汇总,同时,通过表格形式动态展现各个智工业园区的、各个类型、数量的信息。另外,系统以动态滚动的形式,将最新接报的信息展现在最新的列表中。

6.8.2 智工业园区群防群治勤务运行信息

针对各类社会化巡逻防控力量,以智工业园区警务助理、重点单位的安保负责人、保安公司等提供的为主,建立覆盖重点区域的治安巡逻防控网,推进巡逻勤务机制规范化,对这些社会化巡防人员的日常勤务进行汇总及宏观展现。比如：当前全区范围内在勤警力的数量以及备勤警力的数量、当前各单位安保值班领导等。

6.8.3 社会化治安防控实战指挥态势图

充分利用智工业园区警务的社会化群体组织,以警务助理、信息员、重点单位保安等人员为主体,建立智工业园区、社会组织、社会工作者联动机制,在辅助公安警情处置、违法犯罪活动惩治、专项行动过程中强化实战指挥功能,实现跨地的力量调度,分区域、分时段、分作战单元部署任务。以 GIS 地图为依托,支持相关数据如警情、警力、任务、态势在电子地图上实时展示和调度,实现指挥调度扁平化、可视化、智能化、巡防联动等级化、巡防管理精细化。

6.8.4 宏观预警及趋势分析

通过对智工业园区治安情报信息、社会联勤联防信息的分析研判应用,对一个时段的信息进行各种高发趋势、预警、以及同比环比分析等,门户通过引用信息研判分析的服务,对特定专题分析的结果进行展现。通过不同用户的权限控制,让用户可以了解智工业园区治安环境的宏观预警及发展趋势,为指挥决策提供辅助支持。

第七章 智慧工业园区大数据平台规划设计

7.1 需求分析

7.1 .1 采购范围与基本要求

建设 XX 高新区开发区智慧园区的人口库（1 2 万居民）、法人库 （1 *** 家企业 ）、地理信息库 （ 已建设区域 35 平方公里的 3 维电子地图、未建设区域 80 平方公里的航拍电子地图 ）、视频库(1 000 个摄像点)、大数据处理平台、数据管理服务平台。

7.1.2 建设内容要求

7.1.2.1 人口库

人口库的基本信息以公安部门户籍和暂住人口信息为基础，整合人社、计生、园区、教育等多个部门信息资源,建设统一规范的人口库和人口信息服务平台。

(1) 人口库的内容目录

(2) 人口信息服务平台功能需求

数据库层：能够安全存储人口库的内容目录中列出的信息内容,对居民、企业、政府提供安全的人口信息服务,为人口大数据分析提供基本数据源。

应用支撑层：包括门户框架、数据库维护、报表组件、数据挖掘等,用于为应用层提供应用支撑。数据挖掘提供常见的数据分析/挖掘工具、通用算法,利用大数据平台的计算能力进行分析,对人口库数据进行数据挖掘与发现,提供有价值的分析结果。

应用层：包括人口信息服务、人口专题分析、公共服务等。

7.1.2.2 法人库

法人库以工商部门的企业信息为基础,整合各参建部门系统中的法人信息,如机构代码、机构名称、机构类型、经济行业、业务经营范围、机构地址、法定代表人等字段信息,建成标识统一、结构科学、查询快捷、动态管理的法人信息库。制定与交换平台对应的相关标准、制度和规范管理体系,实现工商局、地税局、国税局、质量技术监督局等法人数据相关业务部门之间的网络互联和业务数据的实时交换与应用。

(1) 法人库的内容目录

(2) 法人信息服务平台功能需求

数据库层：能够安全存储法人库的内容目录中列出的信息内容,对居民、企业、政府提供安全的法人信息服务,为法人大数据分析提供基本数据源。

应用支撑层：包括门户框架、数据库维护、统计与报表组件、数据挖掘等,用于为应用层提供应用支撑。数据挖掘提供常见的数据分析/挖掘工具、通用算法,利用大数据平台的计算能力进行分析,对法人库数据进行数据挖掘与发现,提供有价值的分析结果。

应用层：包括法人信息服务、法人专题分析、公共服务等。

7.1.2.3 地理信息库

以国土资源部空间地理数据框架作为基础,采用分布式存储并行计算的技术思路统一搭建地理信息库,再与智慧园区建设涉及的各类专题图层进行融合、关联,实现统一共享,逐渐形成 XX 高新区权威、丰富的地理信息数据库。要求根据不同信息资源类别,提供数据库表结构设计。

地理信息库维护文件主要提供地图基本操作、地图测量、图层控制、空间分析等信息服务功能。

地理信息库配置一套高性能 GIS 工具软件,基于高性能云 GIS 平台搭建,实现空间数据的统一管理,完成空间数据检查、转换、入库、管理、制图显示、服务发布等一系列空间数据分析 处理功能。

(1) 地理信息库的内容目录

(2) 地理信息库管理平台功能需求

数据处理：格式转换、坐标转换、属性编辑、数据裁切。

数据质检：矢量数据检查、栅格数据检查、三维模型数据检查、元数据检查。

入库更新：矢量数据入库、影像数据入库、三维模型数据入库、元数据入库。

数据输出：矢量数据提取、栅格数据提取。

查询浏览：地图浏览、数据加载、SQL 查询、空间查询、数据对比浏览、元数据查询。

历史数据管理：历史版本数据比较、版本数据提取。

系统管理：权限管理、日志管理、备份恢复。

7.1.2.4 视频库

(1) 视频库的内容目录

(2) 视频库管理平台功能需求

与视频监控系统的接口、视频入库、视频目录管理、视频文

件管理、视频特征文件生成、视频检索、视频异常发现等。

7.1.2.5 大数据处理平台

(1) 大数据基础平台

提供基础管控、基础服务的大数据基础支撑功能。大数据基础平台要充分利用目前先进的大数据处理技术,保证系统技术的前瞻性和先进性。大数据基础平台要求提供海量数据的采集、存储、计算、接口服务能力； 需要满足海量、异构的大数据的存储、共享、开放及分析挖掘方面的要求； 需要采用主流的大数据的技术架构,全面满足结构化数据、半构化数据及非结构化数据的存储、处理及计算要求； 提供多种数据采集工具,支持多种格式数据采集； 提供接口服务,供二次开发应用等。

大数据基础平台要求能够管理大数据中心集群的物理服务器资源,控制分布式程序运行,隐藏下层故障恢复和数据冗余等细节,为大数据处理平台提供统一的管理、监控、维护等日常管理功能。主要包括：资源管理、安全管理、运维管理、集群部署及监控、任务调度等功能,同时配备友好的管理界面。

①数据采集要求

大数据处理平台数据主要来自数据资源中心,包括基础库(人口库、法人库、地理信息库、视频库) 数据、主题库 (业务数据库) 数据和互联网数据,同时也支持其他外部系统数据来源。数据采集系统要求提供多种数据采集工具,支持多种格式数据采集。对于结构化数据、非结构化数据以及网络数据采用不同的采集工具进行数据导入。支持多种数据采集方式,比如 ETL、FTP、文件导入导出、关系数据库数据等。

②分布式存储要求

平台能够根据结构化数据和非结构数据的不同特点,分别提供数据仓库和分布式列式数据库存储服务,底层支撑技术支持分布式文件系统,所有的数据可以形成多份副本均匀分布存储在各个服务节点的存储上,保证数据可靠性和提高读写效率。

③大数据计算引擎要求

离线计算引擎 （Mapreduce)：离线分布式计算作为一个海量结构化数据离线处理与分析服务,着力于实时性要求不高的海量数据（TB/PB 级别） 离线处理。支持并行化、容错、数据分布、负载均衡。离线计算引擎需要具有 PB 级的存储处理能力和计算吞吐能力,支持多应用多实例并发同时计算并隔离应用数据和程序的能力。

支持 Mapreduce 等批量数据分布式计算框架。

支持分布式内存计算框架。

支持作业查询预处理调度算法,可根据业务属性对指定的多个队列按照优先级的配置进行任务的提交。

具备高可靠性,支持主控节点双机,避免单点故障不可恢复。

具备高度可扩展,可动态增加/削减计算节点,真正实现弹性计算。

支持离线计算组件界面配置化,可以对配置进行查看和修

改,并立刻生效。

支持离线计算组件性能指标界面可视化,通过界面实时监控组件性能指标。

支持多租户权限管理能力,支持不同用户之间的资源隔离。

支持多应用多实例并发同时计算并隔离应用数据和程序的能力。

内存计算引擎（Spark ）：基于内存的迭代计算框架,适用于需要多次操作特定数据集的应用场合。由于中间输出和结果可以保存在内存中,从而不再需要读写分布式文件系统,能更好地适用于数据挖掘与机器学习等需要迭代的算法。

支持作业查询预处理调度算法,可以根据业务属性对指定的多个队列按照优先级的配置进行任务的提交。

支持审计日志可查询,在管理运维的界面中可以进行内存计算引擎日志的查询。

支持相关存储目录规整,对内存计算引擎的数据目录进行规整,修改默认配置,并提供界面上的修改配置的地方。

支持配置界面化,能够在管理运维界面上对内存计算引擎的配置进行查看和修改,并能够同步到前台立刻生效。

支持通过界面展示性能指标,能够在界面上查看内存计算引擎的性能指标数据。

支 持 on Yarn 等方式,在管理运维界面上安装服务,可以在安装的时候,选择 On Yarn 等的方式安装。

支持内存计算引擎的 Master 的 HA 等,可以对内存计算引擎的 master 角色进行 HA 等部署,以保证该节点的高可用性。

实时计算引擎（例如 spark streaming、Storm）：实时分布式计算需要提供大吞吐量的实时流式数据处理。要求保证高可靠性的前提下让数据处理更加实时,具备低延时、容错和分布计算特性。采用分布式计算框架提供实时计算服务,可按需扩容。

支持高并发低延时的数据处理。

计算引擎：支持 SPARK STREAMIN 等 G 实时计算框架、STORM 分布式流式计算框架两种计算框架功能。

支持对流数据的处理,数据可以建立关联处理。

高效处理数据：支持消息的分流、合流、聚合的消息处理。

数据按业务分析,可支持不同的应用接入,并对应不同的应用输出计算结果。

事件监测：对数据处理低延时,满足事件监控等实时性要求很高的场景。

具备高可靠性,支持主控节点双机,具备自动容错能力,避免单点故障不可恢复。

支持实时计算组件界面配置化,可以对配置进行查看和修改,配置修改立刻生效。

支持实时计算组件性能指标界面可视化,通过界面实时监控实时计算组件性能指标。

④全文搜索引擎（例如 solr ）

提供丰富的查询语言,同时实现可配置、可扩展并对查询性能进行优化,提供一个完善的功能管理界面。可以实现集中式的配置信息、自动容错、查询时自动负载均衡、自动分发的索引和索引分片和事务日志等多种特色功能。

可以对搜索引擎集合进行快照,可以周期、定时创建集合快照,对索引数据进行备份。

提供搜索引擎数据切换自动化工具,一键式操作实现搜索引擎数据从一个集群切换到另外一个集群,安全可靠。

提供搜索引擎节点扩容数据重分布自动化工具,搜索引擎节点扩容后数据均匀的重分布到新增节点上,负载均匀的分担到各节点上。

支持搜索引擎服务自动拉起功能,提高可靠性。除管理平台界面手工停止服务之外的异常服务停止后都会自动拉起,保证服务连续可用。

⑤资源管理（例如 yarn ）

资源管理要求能够实现调度和分配集群的内存和计算等资源给上层应用和服务,能够管理运行在集群节点上的任务的生命周期和资源使用,提供静态资源池和动态资源池功能。在多用户运行环境中,能够支持计算额度和访问控制,作业优先级和资源抢占,达到在保障公平的前提下,有效地共享集群资源。支持 VIP 队列管理,支持根据业务需要指定作业在指定的计算节点上运行,隔离重点任务和普通任务,保障重点任务的物理资源。要 求给出详细的设计方案。资源管理能够面向海量数据处理和大规模计算类型的复杂应用提供统一的资源管理和调度。提供通用的并行计算框架,要求兼容批量分布式计算、内存分布式计算、流式计算等多种编程模式。具备高可扩展性,支持作业定点调度，支持优先级高的作业优先分配到资源。能够自动检测故障和系统热点,重试失败任务,保证作业稳定可靠运行完成。

支持作业定点调度,指定作业在哪些主机上运行,隔离重点任务和普通任务。

支持队列增加优先级属性,优先级高的作业优先分配到资源。

支持白名单功能,限制客户端向集群的 resourcemanager 提交作业。

支持提交权限,限制无权用户提交作业并运行。

支持队列属性修改图形化,在图形化界面中配置新增、修改、删除队列属性。

支持队列属性增加“最大作业提交数” 属性,在图形化界面中新增“最大作业提交数” 属性可配置

⑥分布式协作服务（例如 Zookeeper ）

分布式协作服务提供分布式、高可用的协作服务,可以用来构建分布式应用。它能为分布式文件系统、分布式列式数据库、离线计算、资源管理与调度、数据仓库等大数据组件提供重要的功能支撑。在分布式应用中,通常需要分布式协作服务来提供可靠的、可扩展的、分布式的、可配置的协调机制来统一各系统的 状态。

帮助系统避免单点故障,建立可靠的应用程序。

提供分布式协作服务和维护配置信息。

⑦安全管理

安全管理能够提供以用户为单位的身份认证和授权,能够对集群数据资源和服务进行访问控制,包括系统用户、应用用户的身份和权限管理,日志管理等。

⑧运维管理

主机管理：可以对已经添加的主机及其运行状态进行查询，可以对单台主机进行全面监控。通过在已添加主机安装代理,支持通过代理访问计算集群提供相关组件服务和操作。要求给出详细的设计方案。

服务管理：对大数据平台包含的各个组件服务提供的管理界面,可对各组件运行状态进行监控,可执行启、停操作； 除手动停止服务外,系统监测到服务异常终止时可以自动拉起服务,并可以根据需要打开或关闭自动拉起开关。可对具体角色实例进行管理。为避免应用之间在申请组件服务时相互干扰,提升应用的健壮性和可靠性,应支持相同组件的服务既共享物理资源,又相互独立。要求给出详细的设计方案。

告警管理：告警管理功能包括告警查看、阀值设置。监控系统各类异常,在管理界面上实时呈现。支持集群内不同节点差异化告警阈值设置。

系统管理：包括系统配置、巡检、备份。其中,系统配置包含版本设置和 SNMP 设置。巡检功能需要支持自动巡检和手动巡检两种方式。提供备份功能,包含快照和集群间备份。支持服务日志级别动态调整,支持组件配置项快速查找功能,并且用户可以根据需要新增自定义组件配置项。

⑨展现界面设计

详细展示大数据平台的运行情况。界面展示内容包括主页界面、集群界面、主机管理界面、告警管理界面、安装界面、系统管理界面、日志界面、安全界面等。

主页界面：可以整体查看集群的整体运行状况,包括主机、服务等资源的数量、在线情况； 运行负载情况； 以及告警信息。

集群界面：包含服务管理、静态资源池、动态资源池等； 其中,服务管理界面提供对大数据平台各组件运行状态进行监控，可执行启、停操作； 静态资源池界面和动态资源池界面可对根据服务状态对资源进行静态和动态调整。

主机界面：可以查询已添加的主机及其运行状态,也可对单台主机进行全面监控。

告警界面：主要包含告警查看和阀值设置。

安装界面：包括安装集群、安装主机、安装服务、机架管理、升级服务、升级主机。

系统管理界面：包含巡检报告、开关设置、版本设置等内容。

日志界面：分为操作日志、系统日志、安全日志。可以按照

查询条件对日志进行查询操作,并可对日志可以进行分类、删除、过滤、导出。

安全界面：包含部门管理、用户管理、角色管理等。

⑩集群部署及监控

集群部署与监控能够提供整个云操作系统以及上层应用服务的部署、配置管理以及服务的自检和自举。

集群部署：支持自动化的安装部署,使用工具进行自动安装，简单快捷。主要功能包括：集群安装、主机安装、服务安装、服务升级、主机升级、机架管理。

运行监控：可以整体查看大数据集群的整体运行状况。包括主机、服务等资源的数量、在线情况； 运行负载情况； 以及告警信息。同时监控大数据平台各组件运行状态、硬件资源占用情况（硬盘、CPU、内存等） 等,如果被监控对象出现异常情况,监控系统就会在相关管理告警页面发出告警通知。

(2) 大数据多维分析查询系统

①总体要求

大数据多维查询系统要求提供超大数据规模数据查询,支持 PB 级数据量。针对海量数据可以进行任意维度的密集计算与检索,支持建立 OLAP Cube,提供 MOLAP 能力。支持高并发、低延时的在线数据应用系统,能够提供高并发的实时计算查询服务 ,对于百亿行级别的数据可在亚秒级时间返回查询结果。大数据多维查询系统主要面向传统架构中 OLAP（联机分析处理） 数据访问场景,利用多维分析技术,针对特定分析主题,设计多种可能的观察方式,设计相应的分析主题结构,使用户在多维模型基础上进行快速、稳定、交互式访问,以达到复杂分析和数据预测的作用,实现实时联机分析处理的效果,面向高并发、海量、低延时的业务场景。

②创建数据模型

系统能够根据维度和指标的要求,从现有的数据表中选择可对应维度或指标的字段,将这些字段的信息分别保存在维度表和度量表中。支持层级维度、联合维度、可推导维度等维度降维优化技术。根据业务的聚合需求,支持定义度量的聚合形式,包括 SUM、MIN、MAX、COUN、T COUNT_DISTINC 等 T 。可定义分区类型、分区列和开始日期等,以支持采用增量构建方式对 Cube 进行构建。

③分析查询处理

系统能够根据维度指标定义及关联关系,提供多维数据的分析查询处理,在查询过程中能够分别根据上钻、下钻、切片、切块、旋转、TOPN 等操作进行相应的处理。

支持 web 页面向导式模型构建及任务监控。支持 ANSI SQL 查询标准,对外提供标准的 ODBC、JDBC 驱动及 RESTAPI 接口。

(3) 大数据智能分析系统

①总体要求

大数据智能分析系统提供各类数据的融合与共享服务,要求集成丰富的数据挖掘算法,能够对海量数据提供高效的分析和计算。数据分析挖掘引擎支持并行化统计算法和机器学习基础算法库,支持的并行化基础算法,能够处理大数据集。

②算法库

大数据智能分析平台,需集成丰富的机器学习、数据挖掘算法,包括但不限于分类、预测与回归、聚类、降维、推荐/协同过滤、相似度等算法,支持对海量数据进行高效的分析和计算， 支持图计算和图挖掘,支持用户扩展算法库。

聚类分析：集成常用的聚类分析算法对数据进行抽象的分组分类。

分类分析：在设定好的分类之中,对数据进行归类。

关联分析：集成常用关联分析算法,对数据之间的关联关系进行分析,得出不同数据之间的关联关系。

回归分析：集成常用回归分析算法。

特征分析：集成常用特征分析算法,挖掘数据潜在的特征。

图挖掘：基于图和图并行计算框架提供图挖掘工具,主要包含：连通图、最短路径、三角关系计数、社区关系。

③智能分析系统

数据准备：通过对业务需求分析，搜索所有与业务对象有关的内部和外部数据信息，从中选择出适用于数据挖掘应用的数据，并进行数据预处理。数据预处理可以加快分析过程，提高分析结果的精度，针对不同的数据类型缺失值的处理各不相同，需要结合业务场景。

数据探索：通过统计分析和关联分析等手段，能够深入挖掘多源多维数据之间的关联性，从不同的维度分析数据，加深对数据的理解，提取可能对业务结果相关的影响因子，探索发掘数据的内在规律特征，为分析模型对业务进行定量与定性的结合分析。

数据构建：根据数据源类型、业务要求建立对应的数据模型。通过分类、聚类、关联、回归、特征分析等机器学习算法和分析方法，对海量多样化数据进行进行模型构建和数据分析挖掘。数据模型的设计包括设计和准备数据源，数据的处理，选取和设计数据算法。数据模型的建立是一个预定义、评估、优化的过程。

模型评估：利用评估算法对模型进行评估，评估数据分析结果的合理性、合法性，评价模型的优劣。根据分析结果及时调整和优化数据模型，如果结果不符合预期，需要调整参数进行机器学习，重新估算。

可视化智能分析工具：要求提供可视化智能分析工具，加速数据分析模型设计。可视化智能分析套件为数据分析提供直观的图形化用户界面，用于设计分析流程。实现完整的建模步骤，从数据加载、汇集、到转化和准备阶段，再到数据分析和产生预测阶段。

7.1.2.6 数据管理服务平台

数据管理服务平台是一个管理、展现平台，主要包括：数据治理与监控系统、数据服务集成管理系统和大数据展现门户等。

（1 ）数据治理与监控系统

数据治理与监控系统是一个数据治理和数据监控的综合管理系统，对数据资源中心和大数据处理平台两大部分数据进行治理和管控。数据治理按照数据全生命周期来管理，要求包含：数据源管理、数据质量管理、数据地图管理、数据血缘管理、数据安全管理和元数据管理等； 数据监控与数据治理相辅相成，实现对数据资源的全程监控，包括：全局数据监控、部门数据监控、数据存储使用监控和数据异常监控等内容。

①数据标准管理

术语标准管理：包括限定词、同义词、术语等信息库的管理。

元数据管理：元数据记录了数据源的结构信息，有了元数据才能对数据源进行各种操作，元数据管理需要提供对各数据源的元数据进行注册，加载，查看等功能。

数据源管理：数据源管理包括：基础环境的管理、标准编码管理等。

基础环境管理：基础环境配置管理用于进行一些基础信息的配置，包括：源、目标数据源的配置、标准数据库表结构配置及其编码表的配置等。

②标准编码表管理

用于对数据中心数据涉及的编码表及其编码项进行定义。

③数据处理管理

提供完善的数据处理功能,如数据清洗、数据比对、数据加载、数据转换、数据共享等功能。

④数据规则与质量管理

数据质量监控是根据预设的规则来检测数据中的质量问题,检测规则可自主配置,也可以自主编写规则表达式。数据质量监控与系统调度关联使用,发现脏数据,避免错误的数据流入下游应用。

⑤数据地图

数据全局视图:展示从外部源到内部库,到输出数据库的数据整体流向,展示类别数目、库数目、表数目、分别统计库、表、字段、作业、任务等数量。从表数目和数据存储量的角度展示数据库中按月 度变化的动态信息,以直观的图形化进行动态展示。

并且可以区分不同部门进行统计。

数据动态分布:从表数目和数据存储量的角度展示数据仓库中按月 度变化的动态信息,以直观的图形化进行动态展示。并且可以区分不同部门或者租户进行统计。

数据血缘:数据血缘以历史事实的方式记录每项数据的来源,处理过程,应用对接情况等,记录了数据表在治理过程中的全 血缘关系。数据血缘就是通过对数据处理的全过程追踪,找到以某个数据对象为起点的所有与该对象相关的元数据和它们之间关系的一种技术手段。

(2) 数据服务集成管理系统

搭建基于企业服务总线(ESB) 的服务集成管理系统,构建数据服务的统一通信通道,即使在协议不同、格式不同、标准不同的情况下,服务与对接服务之间都可以实现交互通信,传递消息,以便实现服务集成管理目标,从而实现各类数据服务的统一管理,面向政府用于、企业、公众、开发者,提供便捷的数据服务。具体包括:

①服务注册与发布

提供服务定义、注册、审核和发布功能,发布前可以对服务的配置参数进行审核与修改,配置通道,发布后,自动生成/更新对应服务的配置文件(如 WSD)L,连同服务参数配置,更新至服务目录中;提供对注册/发布服务的连通性测试;

②服务生命周期管理

提供服务的注册、变更、下线的申请、审核、复核功能,检查和确认服务状态以执行变更、下线;根据服务优化管理中的服务拓扑分析,调整服务层级分类或整合服务,以实现优化; 提供服务版本的管理;

③流程管理

支持服务申请、服务变更、服务下线等服务生命周期管理中相关流程的管理功能;

④服务目录管理

提供服务目录的浏览和检索; 提供服务目录/服务定义/服务状态的查询和管理,包括权限的过滤和管理;

⑤接入系统管理

设置和管理服务请求方和接入请求系统的映射关系； 设置和管理服务提供方和接入服务系统的映射关系； 设置和管理服务请求方、服务提供方在服务治理系统的用户映射关系；

⑥接口数据管理

提供数据字典的定义和管理,提供服务方法接口和数据字典字段的映射关系设置。

(3) 大数据展现门户

大数据展现门户是智慧园区大数据中心对外服务窗口,门户包括两个方面：政务数据资源门户（内部数据门户） 和公众数据门户（外部数据门户） 。

政务数据资源门户作为大数据管理部门信息发布和资源服务的总管理入口,为各级政府部门提供信息资源展示、在线信息服务、信息检索、系统集成访问等功能。另外,针对系统管理员、各级领导、政务用户的不同应用需求,提供个性化工作台。

公众数据门户提供政务部门可公开各类数据的下载与服务，为企业和个人开展政务信息资源的社会化开发利用提供数据支撑,推动信息资源增值服务业的发展以及相关数据分析与研究工作的开展。

①政务数据资源门户

门户基本管理：政务数据资源门户主要是提供政务大数据中心数据成果的展示和应用访问入口的应用集成。提供单点登录、访问权限管理,后台内容管理等功能。

在线查询服务 :针对政务数据中心,开发高效率的在线查询服务。人口信息、法人信息、宏观经济、信用信息等面向政府部门提供信息服务,空间地理信息服务包括地图基本操作、地图测量、图层控制、空间分析以及相关数据融合等信息服务功能。

信息资源综合展示：能通过可视化的方式展示区域内信息资源的全景,即：部门信息资源的分布情况,需求情况、使用情况， 需要按照不同视角进行呈现,要求包含但不限于：资产总体视图、组织机构视角、服务对象视角、信息资源视角、协同主题视角。

用户交流模块：为用户提供交流的手段,每个授权用户都可以在交流板块上提出问题、见解或者是进行讨论,针对交流的问题可以选择是否公开。

用户帮助模块：为用户提供平台功能及其操作方法的介绍和帮助说明,使各级用户尽快掌握使用方法。

②公众数据门户

为了实现政务数据对社会的开放,带动大数据产业发展,利用政务大数据促进信息产业创业创新,建设数据对外开放的门户,实现政务大数据的对外开放。针对公众数据门户将要充分利用政府门户网站,在现有的门户网站上开辟一个政务数据开放的入口,点击后即可进入公众数据门户。公众数据门户的主要功能有：资源目录、数据开放接口、APP 应用、互动交流等。

资源目录：社会公众可以通过资源目录查找到需要的数据，找到相应数据的获取方式,数据可以是通过下载方式获取也可以通过数据接口的方式获取,无论哪种方式都需要用户注册认证后才可以获取。用户可以通过数据资源主题的方式查找,也可以用户数据来源各部门的方式查找。

数据开放接口：用户可以通过此功能查找到可以调用的数据接口，并可以查找到数据接口的调用方式、说明文档、代码示例等相关内容，通过功能应用开发人员可以方便的通过数据接口获取所需要的数据。

互动交流：互动交流功能是网站用户与网站管理人员进行互动交流的模块，在这里网站管理人员可以将网站的使用说明和一些常遇到的问题及解决方法公布出来，网站管理人员也可以在此公布调查问卷，征求普通用户的意见。同时，普通用户也可以在这里提出自己的疑问，让管理人员进行解答。

7.2 设计方案

7.2.1 总体平台设计

7.2.1.1 总体架构

智慧园区大数据平台的核心是建立面向宏观经济发展、社会公共服务的数据库和数据服务。总体架构由支撑体系 （标准规范支撑体系、管理运行维护支撑体系、安全支撑体系）、网络系统、信息共享平台软硬件系统环境、数据库体系（中心交换库、基础数据库、主题库、发布库、宏观经济数据库管理系统、元数据库系统）、应用系统（数据交换处理系统、应用支撑系统、数据综合分析系统） 组成.

信息共享平台通过网络收集统计系统和各共建部门的信息资源，并有效地将这些信息资源进行分类整理，实现跨部门、跨行业的宏观经济管理信息共享，并向用户提供数据服务；数据库体系：由元数据控制，实现数据的交换、存储和发布，整合共建单位现有信息资源，构建主题库和发布库，为数据服务提供支持。

7.2.1.2 体系结构图

智慧园区公共基础数据库信息共享平台划分为工作（生产）区、发布（共享） 区和互联网信息发布区。在工作（生产） 区构建宏观经济数据的采集、整合、处理和存储系统； 在发布（共享）区构建宏观经济数据的发布与共享、存储与备份和专网门户系统等环境支撑系统； 在互联网信息发布区构建互联网门户系统，为社会公众提供宏观经济信息服务。

7.2.1.3 总体流程图

智慧园区大数据平台采用在线填报、数据库对接和基于消息的数据交换三种采集方式，集中采集、整合、存储各共建部门指标数据。中心交换数据库存储各共建部门交换来的原貌数据，基础数据库是对原貌数据进行审核转换和加工而成，是主题数据库和发布库构成的基础。元数据库对数据的采集交

换、整合、存储、分析和发布全过程进行定义和约束。专网和互联网的用户可通过门户系统,分别对发布（共享） 区和互联网信息发布区的数据进行访问。

7.2.2 人口基础数据库设计

在没有数据标准的情况下,人口基础数据库数据中心对同一个数据字段可以从多个数据来源采集数据。如：婚姻状态字段可以从计生部门和公安部门采集。对于同一个数据字段,中心对于该数据字段保存多个来源的版本。人口基础数据管理系统提供工具、服务来展现数据的不一致性,数据管理员根据工作制度,对数据字段进行电话等多种手段核实字段的真实数值。中心通过数据

交换系统以数据服务的方式从各业务部门采集数据,保存到公共数据缓存库,使用人口基础数据管理维护系统进行数据比对、冲突检查、数据审核、数据转换。当数据达到一致性、完整性要求时,数据将由公共数据缓存库转存到人口基础数据发布库中，并通过数据交换系统以订阅/发布的方式提供给各业务部门使用。

人口基础数据管理系统维护一个面向对象的公共数据模型， 公共数据模型是公共数据标准规范的实现。公共数据维护系统控制着公共数据的输入和输出,为数据质量把关。人口基础信息综合查询系统采用 B/S 结构,客户端采用浏览器,用户界面是实现不同功能的网页。

综合查询系统的操作页面要求易于使用,使用户能够方便快捷的对网页提供的各项功能进行操作。采用菜单树的方式展开系统的功能。

人口基础信息综合查询系统可以有针对性地,按照用户授权的不同,为不同用户提供不同层次的人口资源公共查询服务。

7.2.2.1 数据接收服务

接收数据的查询是针对各部门交换汇总的信息,进行以部门为单位的信息查询。通过查询工作,可以了解各部门实际提交的信息情况,并实现信息详查和统计工作。系统提供了按部门查询的查询方式。

7.2.2.2 中心数据查询

人口中心数据,就是经过数据比对梳理完成的人口基础信息。针对人口信息量大,涵盖范围广、内容繁杂的特点,在人口基础信息中心数据库设计中,采用信息扩展和关联的方法,逐级分领域和部门展示人口基础信息和扩展信息。

系统根据部门需求进行查询分类,各部门根据本部门业务相关信息进行检索。如公安部门可根据身份证号、姓名、性别、民族为检索条件,进行基本信息的查询； 可根据姓名、暂住证号、身份证

号为检索条件,进行暂住人口信息的查询操作。

其他部门检索与查询操作类似。

7.2.2.3 决策支持子系统

决策支持子系统是根据业务需要,基于人口基础信息,进行数据挖掘,实现统计报表操作,为领导决策提供快速的报表支持。

7.2.2.4 授权管理

授权管理,就是提供信息需求部门申请查询授权,信息提供部门审批授权的功能。

申请部门选择对应的信息表,向信源部门提出申请; 信源部门根据业务规则,对申请部门提供授权或不授权,此外,授权功能提供时限控制和授权使用次数控制。

7.2.2.5 设计方案

数据比对系统通过数据比对引擎,实现对人口基础信息的比对工作。

依据的业务需要,数据比对包括比对操作,各部门数据的过滤查询,各部门信息比对入库结果查询。人口基础信息的比对, 依据其特点,采用自动比对和人工参与比对结合的方式,实现基础信息的比对功能。

数据过滤查询是针对部门提交的数据,进行梳理过滤与清洗,得出的清洗出的问题数据进行查询操作。

与数据过滤查询类似,数据入库查询是将部门信息与人口基础信息总表信息进行比对,并经过相关部门审批确认,比对出现差异错误信息的查询。

7.2.2.6 信息核验

结合比对系统人工比对功能,提供部门提出比对结果意见功能。当部门业务信息进入比对系统后,如出现基础信息库和业务应用源头部门信息不匹配,需要业务人员参与的情况下,提供业务部门信息核验功能。

7.2.2.7 系统管理

系统管理功能是实现对使用人口基础信息查询系统的用户进行管理。人口基础信息综合查询系统提供用户、角色、权限的设定。

即每个申请的用户,根据其角色,享有角色指定的权限。系统管理员可以根据用户情况,赋予固定

角色。

系统管理员可制定新增用户指定角色以及分配权限。

系统管理分为用户管理和角色管理。

（1） 用户管理：管理系统用户,以及给系统用户分配角色和权限。

（2） 角色管理：角色管理是对每个角色进行查询,并分配相应权限,系统管理员可以根据角色权限,以及每个用户的允许查询权限为用户授权。

7.2.3 法人基础数据库设计

法人基础数据库系统实现法人基础数据查询、统计和管理等功能的应用系统。

7.2.3.1 系统管理

管理系统用户,以及给系统用户分配权限,其中包括用户角色管理、角色信息管理、部门账户管理、系统日志管理、系统网络布局查看以及部门交换频率查看。

7.2.3.2 授权服务

法人基础数据库系统设计原则遵循 “谁提供谁维护” 的原则，在中心形成的法人基础数据库中的法人信息,对于公开开放的数据,不需要经过部门授权就可以查看,但对于部门未开放或者指定对象开放的数据,其他部门需要查询该部门的数据需要向数据提供部门提出申请,在申请通过后,才可在授权允许的范围内进行查询。

授权服务主要功能包括：

（1） 数据授权管理：通过申请查看授权向数据提供部门提出查询申请,信息所属部门可以对其他部门对本部门信息提请的查看申请进行审批授权。可以设置授权的查看次数和有效期限，也可以永久授权。

（2） 数据交换申请：如果部门希望其他部门数据交换到本部门,通过数据交换申请向数据所属部门发送申请,申请得到授权后,通过自主交换的方式将数据交换到本部门的指定数据库内。

（3） 共享信息管理：部门设置信息共享的级别,包括：授权开放、公众开放、部门开放等。同时通过信息管理日志查看用户的操作记录,以确保信息的安全。

7.2.3.3 接收服务

提供中心接收到各部门原始数据的查询功能,以及数据的清洗比对功能,具体功能包括：接收数据查看：查询中心接收到各部门发送的原始数据。

清洗比对管理：管理和维护各个部门提供的原始数据的清洗和比对规则。可以增加、删除及保

存规则。在系统后台会根据制定的规则来对接收的数据进行清洗和比对处理。

清洗比对结果：可以根据清洗和比对批次、时间段等条件查询清洗和比对结果,如比对成功和不成功的数据量及所占比例，以及未匹配数据的详细数据和未匹配成功的原因 （如企业注册号

相同,企业名称不同等） 。

手工比对管理：对于通过比对规则比对不一致的数据,通过手工比对管理进行手工比对,比对一致的,通过手工操作更新中心法人信息库,比对仍不一致的,反馈到未匹配数据表,通过交换平台反馈相关部门进行核查。手动比对管理主要解决数据比较特殊,无法制定通用比对规则的数据之间的比对。

部门数据比对：进行部门间的数据比对,如工商有质监无的数据、工商有国税无、工商有地税无、质监有国税无、质监有社保无、国税有社保无等。

7.2.4 信息服务

根据查询条件或者组合条件查询法人信息,返回的结果为清洗比对后的准确数据,对于需要授权的数据,需要先通过授权服务进行授权申请。具体功能包括：

（1） 法人信息服务：查询法人信息,用户也可按条件查询。

（2） 部门信息统计：查看各部门法人信息的数据总量。

（3） 法人码表信息：对于有国家标准的代码表,均会转换成国家标准的代码存入法人基础信息库,如行业类别、法定代表人性别等,对于部门专有的代码表,通过法人码表信息列出,供其他部门下载和使用。

7.2.3.5 统计分析

提供报表统计功能,结合各类基础信息,形成各类报表,提供多种统计功能,辅助领导决策。提供列表、折线图和柱状图等多种展示方式,统计内容主要包括：基础信息统计、行业类型统计、企业类型统计、部门数据差异统计等。

7.2.3.6 地理信息基础数据库设计

7.2.3.7 基础数据

（1） 遥感影像数据

本项目是 XX 高新区主要区域影像数据,建设范围为 30 平方公里。

（2） 遥感影像数据处理

几何校正,正射校正遥感影像在获取过程中,受到如大气吸收与散射、传感器定标、地形等因素的影响,且它们会随时间的不同而有所差异。因此,在多时相遥感影像中,除了地物的变化会引起影像

中辐射值的变化外,不变的地物在不同时相影像中的辐射值也会有差异。

利用多时相遥感影像的光谱信息来检测地物变化状况的动态监测,其重要前提是要消除不变地物的辐射值差异。

数据融合

数据融合实质上是将高分辨率影像空间特征与低分辨率影像多光谱特征组合到一副影像 ， 使得融合后影像即具有高分辨率影像空间特征 ， 又具有低分辨率影像多光谱特征。

数据裁剪与镶嵌

a. 镶嵌

当研究区超出单幅遥感影像所覆盖的范围时,通常需要将两幅或多幅影像拼接起来形成一幅或一系列覆盖全区的较大的影像。在进行影像的镶嵌时,需要确定一幅参考影像,参考影像将作为输出镶嵌影像的基准,决定镶嵌影像的对比度匹配、以及输出影像的像元大小和数据类型等。镶嵌得两幅或多幅影像选择相同或相近的成像时间,使得影像的色调保持一致。但接边色调相差太大时,可以利用直方图均衡、色彩平滑等使得接边尽量一致,但用于变化信息提取时,相邻影像的色调不允许平滑,避免信息变异。

b. 裁剪

影像裁剪的目的是将研究之外的区域去除,常用的是按照行政区划边界或自然区划边界进行影像的分幅裁剪。

图像增强

图像增强是指按特定的需要突出一幅图像中的某些信息,同时削弱或去除某些不需要信息的处理方法,其目的是使得处理后的图像对某种特定的应用,比原始图像更合适。处理的结果使图像更适应于人的视觉特性或机器的识别系统。图像增强主要可分为三类 :频域图像增强方法、小波域图像增强方法、空域图像增强方法。

匀光匀色处理

由于光学遥感影像获取的时间、外部光照以及其他因素的影响 ， 导致获取的影像在色彩上存在不同程度的差异 ， 这种差异会不同程度地影响后续数字正射影像生产、数字城市和数字省区无缝影像数据库建设以及其他的影像工程应用中影像的使用效果。

为了消除影像色彩上的差异 ， 需要对影像进行色彩平衡处理 ， 即匀光处理。

（3） GIS 专题数据库

GIS 空间数据库指的是地理信息系统在计算机物理存储介质上存储的与应用相关的地理空间数据的总和,一般是以一系列特定结构的文件的形式组织在存储介质之上的。空间数据库的研究始于 20 世纪 70 年代的地图制图与遥感图像处理领域,其目的是为了有效地利用卫星遥感资源迅速绘制出各种经济专题地图。

由于传统的关系数据库在空间数据的表示、存储、管理、检索上存在许多缺陷,从而形成了空间数据库这一数据库研究领域。而传统数据库系统只针对简单对象,无法有效的支持复杂对象 （如图形、图像） 。

GIS 空间数据主要有两种组织策略,一种是基于分层的数据组织,另外一种是基于特征的数据组织。基于分层的数据组织是目前常用的也是比较成熟的数据组织策略,基于特征的数据组织是未来 GIS 数据组织的发展方向,但目前还不成熟。本系统就是采用基于分层的数据组织策略,将空间信息分为地图集、图层集和图层。其中系统用到的图层主要有行政图层、道路图层、河流图层、灾害点图层、监测点图层等。在数据管理方面,前端采用 FeatureBase 进行管理,后台采用 SQL Server ***8 很好的解决了网络环境下多用户并发操作、权限管理等诸多问题,同时系统采用多级缓冲机制,大大加快了用户操作地图功能的速度。

矢量数据 :主要是指城市大比例尺地形图。此系统中图层主要分为底图层、道路层、单位层,合理的分层便于进行叠加分析、图形的无逢拼接以实现系统图形的大范围漫游。矢量数据一般通过记录坐标的方式来尽可能将地理实体的空间位置表现的准确无误,显示的图形一般分为矢量图和位图。

图层 :图象都是由一层或多层图层组成。图层功能允许让多张图片进行叠加放置并保存在一个文件中。通过对图像分层放置,您能够有效的把多张图片 混合在一起,隐藏或显示每个单独的图层,文本、绘图和图象可以在各自的图层上被添加、删除、移动和编辑而不会影响其它图层。

地形数据：地形数据是能够表示地球表面高低起伏状态的数据，即具有高程信息的数据。数字高程模型（DEM） 是一种对空间起伏变化的连续表示方法,是一种特殊的 DatasetGrid 数据模型,每个网格的值为高程值,而且有标准的颜色表来表示,这对分幅 DEM 图像的合成很有帮助。

（4） 三维模型

主城区精细化三维建模

本项目主城区精细化三维建模和普通三维建模面积为 30 平方公里。

7.2.3.8 平台建设

1） 基础平台

a. 平台构成

主要由系统软件 （操作系统、网络软件等）、数据库软件 （如 Oracal、SQL Server 等）、GIS 软件平台、应用软件（GIS 二次开发软件、GIS 组件库等） 组成。

b. 基本功能

地图浏览

系统提供地图放大、缩小、平移、鹰眼、全图等基础地图操作, 地图底图服务采用金字塔地图静态缓存切片技术,配合优化后的客户端加载,实现了高效地图刷新,地图操作基本无刷白。

同时在地图数据加载过程中,实时提供进度条显示,方便让用户了解地图数据加载情况。

电子地图具有平滑过渡,使用时不会出现刷白的现象。

图层是地理数据存储的基本单元,图层存储可以是空间矢量数据(如点、线、面) 和属性数据,也可以是一组带地理配准的栅格影像数据,它们都是一组与主题相关的数据单元。

系统提供基础底图图层和专题图层,基础底图可以是矢量二位电子地图,也可以是遥感影线数据,一般作为地图背景数据。

专题图层通常为空间矢量数据,针对不同业务,可以加载一个或多个相关业务专题图层,进行空间属性分析。

数据目录

空间数据目录 ， 是指按照一定的格式和标准,对空间数据资源的基本情况进行描述的目录。根据不同的应用属性,目录以多种形式组织和展开。

基础数据源选择

提供矢量电子地图、卫星遥感影像、DEM 基础数据源数据的目录,提供地图基础底图的切换。

专题数据筛选

提供专题、部门、热门分类的专题数据目录,可自由进行组合叠加。

空间分析

提供针对数据目录中的专题数据进行空间分析的功能,可以实现空间检索和缓冲区检索。

空间检索：提供矩形、圆形、多边形、手绘自由面等多种方式进行空间检索。

缓冲区检索：提供点、线、面基于缓冲半径的缓冲区检索。

数据搜索

图层检索：提供基于数据目录的图层检索,通过指定数据目录中的一个或多个专题图层进行关键字检索。

全文检索：提供基于搜索引擎的全文检索,通过关键字在所有专题图层中进行相关性检索,可以根据词典,提供分词、同义词等方式的模糊检索。

空间标注

点标注：提供基于空间点要素的标注功能,可以实现多种样矢量点和图标点的标注功能。

线标注：提供基于空间线要素的标注功能,可以实现多种样式线符号的标注功能。

面标注：提供基于空间面要素的标注功能,可以实现多种要素面要素的标注功能。

文字标注：提供基于空间点的问题标注功能,可以实现文字自由空间标注。

量算功能

长度量算：提供空间距离量算功能,可以通过多点折线和手绘自由线进行距离长度量算功能。

面积量算：面积空间面积量算功能 ， 可以通过多边形和手绘自由面进行面积量算功能。

地图输出

地图打印：提供当前地图打印功能,将地图输出到打印机进行输出。

地图保存：提供地图截图功能,截图后可保存到剪切板,或者保存为多种格式的图片文件。

2） 空间分析

空间分析是基于地理对象的位置和形态特征的空间数据分析

技术,其目的在于提取和传输空间信息,是利用各种空间分析模

型及空间操作对地理数据库中的空间数据进行深加工,进而产生

新的知识。

a. 缓冲区分析

缓冲区分析是地理信息系统中常用的一种空间分析方法,是对空间特征进行度量的一种重要手段。缓冲区分析是研究根据数据库的点、线、面实体,自动建立其周围一定宽度范围内的缓冲区多边形实体,从而实现空间数据在水平方向得以扩展的信息分析方法。它是地理信息系统基本的空间操作功能之一。从空间变换的观点看,缓冲区分析模型就是将点、线、面地物分布图变换成这些地物的扩展距离图,图上每一点的值代表该点距离最近的某种地物的距离。实际上,缓冲区就是地理目标或工程规划目标的一种影响范围。

b. 叠置分析

叠置分析是地理信息系统中常用的提取空间隐含信息的方法之一,叠置分析是将有关主题层组成的各个数据层面进行叠置产生一个新的数据层面,其结果综合了原来两个或多个层面要素所具有的属性,同时叠置分析不仅生成了新的空间系,而且还将输入的多个数据层的属性联系起来产生新的属性关系。其中，被叠加的要素层面必须是基于相同坐标系统的,基准面相同的、同一区域的数据。

c. 窗口分析

地理信息除了在不同层面的因素之间存在着一定的制约关系之外 ， 还表现在空间上存在着一定的关联性。对于栅格数据所描述的某项地学要素,其中的 (i , j) 栅格往往会影响其周围栅格的属性特征。充分而有效地利用这种事物在空间上相联系的特点,是地学分析的必然考虑因素。窗口分析是指对于栅格数据系统中的一个、多个栅格点或全部数据,开辟一个有固定分析半径的分析窗口,并在该窗口内进行诸如极值、均值等一系列统计计算,或与其它层面的信息进行必要的复合分析,从而实现栅格数据有效的水平方向扩展分析。

d. 栅格数据分析

栅格数据由于其空间信息隐含属性信息明确的特点,可以看作是最为典型的数据层面,通过数学关系建立不同数据层面之间的联系是 GIS 提供的典型功能,空间模拟尤其需要通过各种各样的方式将不同的数据层面进行叠加运算,以揭示某种空间现象或空间过程。同矢量数据多边形叠置分析相比,栅格数据的更易处理,简单而有效,不存在破碎多边形的问题等优点,使得栅格数据的叠置分析在各类领域应用极为广泛。

e. 水文分析

水文分析专题主要是利用地图的基本应用功能以及地图标识功能,对各个水位站的地理位置坐标数据、各个水位站监测到的水情数据在地 图上进行加载,形成一个专题图层,以直观的方式将相关的数据信息集 中显示在一张地图上,以供用户查看和浏览,方便用户对各个水位站的 地理位置以及实时的水情数据等相关信息进行查看。

f. 动态分段

动态分段是在数据库中纪录道路的每种属性的起止点到道路原点的距离,并不是真的将道路切断存储,适合于动态的分析，顾名动态分段。

采用动态分段之后,一个路段（Segment）,是路网上两个交点间连线或者弧的一部分,路段的长

度用其占连线的比例来表示,具有唯一的标识码。在 GIS 数据库中,路段是依附于路网数据,本身没有坐标。由于采用动态分段将道路的各种属性以及其分布集中在一个图层中进行管理,采用线性定位方法,因而容易实现各种“点线” 以及“线线” 的叠加查询分析。

动态分段是对现实世界中的线性特征及其相关属性进行抽象描述的数据模型和计算手段,它可以根据不同的属性按照某种度量标准对线性要素进行相对位置的划分,而对同一个线要素,可以根据不同的度量标准得到不同的相对位置划分方案。

g. 插值分析

在实际工作中,由于成本的限制、测量工作实施困难大等因素,我们不能对研究区域的每一位置都进行测量（如高程、降雨、化学物质浓度和噪声等级） 。

这时,我们可以考虑合理选取采样点,然后通过采样点的测量值,使用适当的数学模型,对区域所有位置进行预测,形成测量值表面。插值之所以可称为一种可行的方案,是因为我们假设,空间分布对象都是空间相关的, 也就是说,彼此接近的对象往往具有相似的特征。

h. 地图裁剪

地图裁剪是从地图矢量数据集合中提取所需信息的过程,它是空间数据处理过程中经常遇到的问题。在进行地形图的开窗、放大、漫游显示和空间目标提取,以及多边形叠置分析时,必须进行数据裁剪。裁剪就是把裁剪区域内地理实体及他们之间的拓扑关系表达出来,可分为两个步骤：一是将区域中的地图元素提取出来,建立矢量数据的简单数据结构； 二是将这些地图元素之间的拓扑关系提取出来,建立矢量数据拓扑关系的表示结构。裁剪后的地图矢量数据不仅含有该区域中各个地理实体的抽象,而且还有对各个地理实体之间拓扑关系的描述,是认识该区域的基础。

3） 拓扑功能

拓扑关系是指空间数据的位置关系。

空间拓扑描述的是自然界中地理对象的空间位置关系,是地理对象空间属性的一部分。在地理对象中涉及的拓扑关系有邻接,关联和包含。这个很容易理解。那么在 GIS 中,运用拓扑有什么好处？拓扑的主要目的是保证数据的质量,提高数据的精度。这也就是在 GIS 软件中,虽然实现的方式不同,但最终的目的无非是保证数据的质量。

地理对象的拓扑关系,主要有以下三种：

相邻 :是指对象之间是否在某一边界重合,例如行政区划图中的省、县数据。

重合 :是指确认对象之间是否在某一局部互相覆盖,如巴士线路和道路之间的关系。

连通 :连通关系可以确认通达度、获得路径等。

4） 网络分析

在 GIS 中,网络分析是指依据网络拓扑关系 （结点与弧段拓扑、弧段的连通性） ,通过考察网络元素的空间及属性数据,以数学理论模型为基础,对网络的性能特征进行多方面研究的一种分析计算。

在 GIS 中,作为空间实体的网络与图论中的网络不同。它作为一种复杂的地理目标,除具有一般网络的边、结点间的抽象的拓扑含义之外,还具有空间定位上的地理意义和目标复合上的层次意义。

具体说来,网络就是指现实世界中,由 和结点组成的、带有环路,并伴随着一系列支配网络中流动之约束条件的线网图形,它的基础数据是点与线组成的网络数据。

网络分析是通过模拟、分析网络的状态以及资源在网络上的流动和分配等,研究网络结构、流动效率及网络资源等的优化问题的领域。对地理网络、城市基础设施网络进行地理分析和模型化,是地理信息系统中网络分析功能的主要目的。

网络分析的基础是网络的建立,一个完整的网络必须首先加入多层点文件和线文件,由这些文件建立一个空的空间图形网络,然后对点和线文件建立起拓扑关系,加入其各个网络属性特征值,如根据网络实际的需要,设置不同阻强值,网络中 的 连通性,中心点的资源容量,资源需求量等。一旦建立起网络数据, 全部数据被存放在地理数据库中,由数据库的生命循环周期来维持其运作。

地理信息系统中的网络分析就是对交通网络、各种网线、电力线、电话线、供排水管线等进行地理分析和模型化,然后再从模型中提炼知识指导现实,从网络分析应用功能的角度上,网络分析划分为路径分析、最佳选址、资源分配和地址匹配。

在路径分析中有以下几类的分析处理方向:

静态最佳路径:由用户确定权值关系后,即给定每条弧段的属性,当需求最佳路径时,读出路径的相关属性,求最佳路径。

动态分段技术:给定一条路径由多段联系组成,要求标注出这条路上的公里点或要求定位某一公路上的某一点,标注出某条路上从某公里数到另一公里数的路段。

N 条最佳路径分析:确定起点、终点,求代价较小的几条路径,因为在实践中往往仅求出最佳路径并不能满足要求,可能因为某种因素不走最佳路径,而走近似最佳路径。

最短路径:确定起点、终点和所要经过的中间点、中间连线, 求最短路径。

动态最佳路径分析:实际网络分析中,权值是随着权值关系式变化的,而且可能会临时出现一些障碍点,所以往往需要动态地计算最佳路径。

资源分配主要是优化配置网络资源的问题,资源分配的目的是对若干服务中心,进行优化划定每个中心的服务范围,把所有连通 都分配到某一中心,并把中心的资源分配给这些 以 满 足其需求,也即要满足覆盖范围和服务对象数量,筛选出最佳布局和布局中心的位置。资源分配网络模型由中心点 (分配中心) 及其状态属性和网络组成。分配有两种方式,一种是由分配中心向四周输出,另一种是由四周向中心集中。这种分配功能可以解决资源的有效流动和合理分配。

选址功能是指在一定约束条件下、在某一指定区域内选择设施的最佳位置,它本质上是资源分配分析的延伸,例如连锁超市、邮筒、消防站、飞机场、仓库等的最佳位置的确定。在网络分析中的选址问题一般限定设施必须位于某个节点或某条 上,或者限定在若干候选地点中选择位置。

地址匹配实质是对地理位置的查询,它涉及到地址的编码。

地址匹配与其它网络分析功能结合起来,可以满足实际工作中非常复杂的分析要求。所需输入的数据,包括地址表和含地址范围的街道网络及待查询地址的属性值。

5) 海图数据

电子海图 (Electronic Chart ,EC)是用数字形式表示的以描写海域地理信息和航海信息为主的

海图,它与国际海上人命安全条约 (SOLAS)所需要的纸质海图等效,电子海图亦称为数字海图(Digital Chart) 。它同时是一个内容、结构、格式均标准化了的数据库,这个数据库由官方授权的权威航道测量部门制作发行,供 ECDIS 使用。

电子海图的结构一般分为电子海图目 录、物标分类编码系统、用户数据格式的 ENO、ENC 改正数据库、海图图式符号库、用户数据库、航海信息咨询系统数据库等主要部分。

电子海图目录：ENC 中存储的海图,一般要根据比例尺（全球图、沿岸图等） 的不同划分成几个比例尺级别。如我国海区可以划分成 1 ：1 00 万、1 ：25 万等几个比例尺级别。为了有效的使用海图数据,必须摒弃原纸质海图图幅的限制,将每级比例尺的海图所覆盖的整个区域划分成大小合适的单元,对两幅纸质海图重叠的部分只取一次数据。

6） 三维分析

GIS 的优势在于能够直观直接地展示复杂的地理信息,同时具有强大的空间分析功能。三维 GIS 突破了空间信息在二维平面中单调展示的束缚,可以更加准确真实地展示现实环境,为信息判读和空间分析提供了更好的途径。某些特定的分析功能,如地质分析、日照分析、空间扩散分析、通视性分析等高级空间分析功能仅能在三维 GIS 中实现。

三维 GIS 是模拟、表示、管理、分析客观世界中的三维空间实体及其相关信息的计算机系统,能为管理和决策提供更加直接和真实的目标和研究对象。

三维 GIS 的实现关键在于三维数据模型的建立。对空间实体及空间关系的准确、有效表达是三维空间建模的主要任务,它应具备以下功能：空间实体及空间关系的定义及描述与表达方法，空间实体和非空间实体之间的直接或间接关系的描述与表达、空间数据操作的分类定义及操作符号和操作规则描述、空间实体和非空间实体之间的相互制约机制及限定时间序列下的动态变化，空间数据的完整性及一致性检验规则等,目前提出的三维空间数据模型可分为 3 类,即：面模型、体模型和混合模型等。

7） 三维特效扩展

在基于三维可视化场景中,最基本的空间查询是空间点的三维坐标查询,它是其他交互操作和空间分析的基础。由于消隐处理,计算机屏幕上的三维模型的像点与三维模型的大地坐标不是一一对应的,必须确定鼠标点捕捉到 2D 屏幕坐标所对应的 3D 大地坐标才能进行正确的空间分析和查询操作,这实际是将计算机的 2D 屏幕坐标反解为 3D 空间坐标,是透视投影的逆过程。

通视分析是以某一点为观察点,研究某一区域通视情况的地形分析,属于对地形进行最优化处理的范畴,通视功能的实现是指一个视点在多个方向上的可见性。它的算法原理是从 DEM 中的某个像素向周围像素发出一系列射线,并计算从视点 A 到周围每个像素 X 的坡度角,若此坡度角大于已有坡度角中的最大角,则像素 X 是可见的,否则不可见。

7.2.3.9 GIS 平台

（1） 海量数据管理

支持元数据的定义,可以创建、编辑和管理元数据。

系统基于 OGDC 标准（Open Geo-DataBase Connectivity ，开放式空间数据库连接标准），实现了无差别访问多种数据来源，将不同平台的不同格式数据加载到同一个场景中展示,包括矢量、栅格、影像、栅格目录、文本注记、网络、三维矢量、多分辨 TIN 等数据类型。支持业界先进的数据模型 Geodatabase。

系统的数据引擎支持的数据格式,支持 WM、S WFS、WM、SKML\KMZ 等标准格式数据和编目服务（Catalog Services）等，提供对 OGC 地图标准的广泛支持。支持任意等级建立影像数据金字塔以及金字塔的部分更新,支持 LZW、JPEG、JPEG***0 等压缩技术存储影像。

系统支持多种矢量数据存储格式,有 OGC 的 ST_Geometry 格式、SQL Server 的 Geometry 和 Geography 格式。支持 OGC 空间 SQL 语句直接访问矢量数据。

系统直接支持 ENVI 的文件格式,可直接读取、显示 ENVI 格式。

系统保证在 DBMS 中存储矢量数据的空间几何完整性,支持属性域、子类,支持定义空间数据之间的规则,包括关系规则、连接规则、拓扑规则等。

系统支持多版本数据管理技术。支持多用户并发编辑和访问。支持多级树状结构的地理数据模型级别的数据库复制和同步技术。

系统提供平台级（非二次开发） 的角色服务安全访问控制 LDAP,Token Service 认证。

系统支持使用 python 脚本调用来完成地理空间数据的处理和分析。

（2） WebGIS 功能

系统支持对二维/三维场景进行各类漫游操作：放大、缩小、平移、倾斜、旋转量算、视图回溯、图层控制等操作。

系统支持基于 Web 的在线地图数据编辑,包括点、线、面的空间数据编辑和属性编辑,支持多用户并发编辑。

系统支持基于 Web 在服务器端实现高级 GIS 分析功能,除了二维地图显示外,还包括三维地图显示、高级 GIS 空间分析（叠加分析、邻近分析、数据管理） 等。

系统提供 GIS 服务创建和管理框架,支持便捷的创建和管理二维/ 三维地图显示服务,影像服务,要素服务,搜索服务,几何服务。

系统提供免费的、可定制的三维数字地球客户端,可访问并使用服务器平台所发布的 GIS 服务,如三维 GIS 服务、在线 GIS 分析服务。

系统软件通过了 OGC 认证,支持发布各种开放数据格式,如 WM、S WFS、WCS、KML 等； 并提供针对 WMS 的 SLD 支持。

系统提供 GIS 服务的创建和管理框架,基于此框架可以很方便地创建和管理二维/三维地图显示服务,索引查询服务,要素编辑服务,OGC 服务,远程空间数据库访问服务,地理定位服务，和自定义高级 GIS 分析服务、遥感影像服务。

系统支持发布搜索服务可对企业内的 GIS 内容和文件夹进行索引查询,支持用户快速查找。

系统提供交互式数据下载功能的 GIS 分析工具,支持数据压缩并通过电子邮件发送数据。

系统提供几何形状运算服务,支持动态计算自动闭合、凸多边形、裁剪、加密、求差、距离、综合、相交、偏移、重塑、截断/ 延伸、组合。

系统支持时态感知图层,存储数据集某时间段的状态信息。

发布地图服务时,保留时态信息,并可通过地图服务访问。基于时态信息,可改变地图的显示或进行时间查询。

系统支持要素附件,提供了地图上地理要素相关的附件上传和关联的方法。附件例如 Txt、PDF 和图像文件,包含要素的补充信息。当发布地图服务后,客户端可查看和下载附件。

系统支持发布影像服务,提供多种客户端控制设置,如每次请求的最大影像尺寸、每次镶嵌的最大栅格数、默认重采样方法、压缩方法、镶嵌方法、每次请求返回最大记录数、每次请求最大下载数。

系统支持缓存地图与动态地图叠加使用功能,相对固定的数据：采用缓存地图方式,大大提高效率； 动态数据：采用动态地图方式,便于信息处理。支持将多类型、多精度影像、地形叠加分组分层显示例如：可支持影像数据集、SIT、GeoTif、WM、S web 地图缓存、文件缓存等多种数据存在形式,支持不同范围、不同投影、不同分辨率的影像叠加显示,支持图层的叠加、半透明显示,图层顺序控制、可见性控制等。此外,还支持各种海量矢量数据、三维模型数据的叠加显示,矢量数据的显示无需进行预处理且具有高效、依地形显示的特点。

系统支持多种缓存格式:凑缓存格式将所有切片打包成大的 Bundle 文件,而不是将单个切片存储成单个文件； 混合模式缓存支持在同一缓存中使用不同图片格式的切片。

系统提供协同缓存创建工具,支持缓存切片的导入和导出。

系统具有开放性特征,能用国际上通用的多种主流开发语言实现应用的开发,并预留了接口。支持 COM、.NET、J2EE、Flex 、Silverlight ； 系统提供多种开发框架,例如 Java ADF、.Net ADF、Flex、Silverlight、JavaScript 等。

系统提供基于 IOS、Windows Phone 和 Android 平台的 API,具有良好的可扩展性、支持 Java、C#和 Objective-C 开发。

系统免费提供多个可配置的 Flex、Silverlight 富客户端应用程序模板和插件,简化开发。

系统能调用 Virtual earth 地图和 Google Map 地图,提供全球免费底图地图服务。

系统提供的 LOD 技术支持多层地理、地质、环境等海量二、三维数据的动态加载,支持海量矢量数据的快速显示,提供丰富多样的表现形式,使矢量数据与三维叠加达到理想效果。

系统可以按指定的点与点之间或者矢量线进行飞行显示、矢量数据的浏览,实现二维和三维空间数据、属性报表和影像之间的联动浏览查询,在浏览飞行进程中实现定位、放大、缩小等漫游操作,可以设定观察高度、飞行速度、方向角、显示的水平比例尺高程比例尺等参数信息,可以设定山洪、地理、行政、环境等其他相关的矢量信息在漫游图形上加载显示； 可在影像上进行业务信息的标注接,具备无限的关联空间；

系统提供鹰眼控件、图层管理控件和图例控件、地图基本操作控件等辅助工具。把它们与 WebControl 等主要功能控件绑定后,不用编写任何代码就能直接实现相互间的连动。

（3） 远程数据代理功能

通过远程数据代理,可实现对标准的 WM、S 的空间数据共享、集成。

WFS 等 OGC 标准

数据是 GIS 的灵魂,GIS 的空间数据有着和传统 GIS 并不相同的使用模式。特别是在互联网提出 Web2.0 概念并在互联网应用上取得重大发展的时候,分布式框架下的空间数据也应当引入一些崭新的概念和应用。下面在分布式 GIS 框架下分别从数据的访问、分析、编辑和搜索 4 个方面探讨它们的重要功能与特点。

空间数据的共享访问。分布式 GIS 的各个节点的空间数据虽然是异构的、非标准的,但是在分布式框架下,这些过去的困难都不是问题,因为节点内部对于用户来说是透明的,另外,元数据的共享也在一定程度上提高了空间数据共享的准确性和明确性。

支持 ESRI,ArcGIS ,ArcGIS Server ,SuperMap,MapGIS 的数据访问。

在分布式计算模式环境中 ， 无论是硬件平台还是软件平台都不可能做到统一。而大规模的应用软件通常要求在软硬件各不相同的分布式网络上运行。为了克服这种局限性 ， 更好地开发和应用能够运行在这种异构平台上的软件 ， 迫切需要一种基于标准的、独立于计算机硬件以及操作系统的开发和运行环境， 中间件技术应运而生。采用中间件是介于应用系统和系统软件之间的一类软件 ， 它使用系统软件所提供的基础服务 （ 功能 ）， 衔接网络上应用系统的各个部分或不同的应用 ， 达到资源共享、功能共享的目的。

7.2.4 视频基础数据库设计

7.2.4.1 建设规划

视频图像信息数据库是一个提供除传统连续视频流以外的视频图像内容信息流的存储和相应服务的基础视频资源库,是一个提供除传统视频监控实时浏览、云镜控制、录像下载回放等基本功能以外的、与公安实战应用能深度结合的视频图像信息资源系统。

视频图像信息数据库有广义和狭义之分,广义上的视频图像功能共信息数据库涵盖所有用于存储视频、图像及其结构化描述信息等内容的存储系统,包括目前用于存储连续视频流的存储系统。狭义上的视频图像信息数据库指用于存储视频监控设备自动抽取或人工采集和标注的视频片段、图像、索引、标签、视频结构化描述信息的数据库,如卡口图像和车辆通行信息、案/事件信息等。

视频库建设主要针对 XX 高新区开发区智慧园区视频监控系统产生的视频图像信息 ， 进行统一的存储和管理,利用大数据视频分析技术提取视频文件特征值,及时发现视频文件中的异常信息进行预警研判等。

7.2.4.2 设计方案

XX 高新区智慧园区视频图像信息数据库系统指用于存储视频监控设备在事件触发下自动抽取,或人工值机和现场巡查、以及案件研判过程中采集和标注的视频片段、图像、索引、标签、视频结构化描述信息的数据库,以及支撑视频图像信息对象应用的相关服务功能。

2 视频特征 视频特征文件

视频图像信息数据库系统存储 XX 高新区开发区智慧园区视频的核心信息和部分特征信息,主要包括视频目录管理、视频文件管理、视频特征文件生成、视频检索、视频异常信息等。

视频库采用数据同步更新等策略保持数据库一直处于热备状态,有效的保证平台运行的稳定性。

1) 逻辑结构

视频库结构从逻辑概念上主要分为如下几个部分:

管理模块

主要包括管理用户、权限等信息表。

内容模块

主要包括视频目录、视频文件、视频检索等信息表。

日志/ 事件模块

主要包括管理用户日志、故障通知、报警事件等信息表。

特征模块

主要包括视频特征文件信息、视频异常信息等的信息表。

2) 访问模型

视频图像信息数据库由于职能定位不同具体建设方式与 XX 高新区开发区智慧园区已有的视频监控系统数据库有所不同,但是数据库接口应该一致。

由于传统的 SQL 数据库技术已经难以满足大数据、结构化非结构化混合数据等应用的需求,当前各类 NoSQL 数据库和云数据库等技术发展非常迅速,所以本技术不具体规定数据库内部的具体表结构的实现,而是从数据库访问接口操作以及操作对象角度去制定相应的协议。

从系统总体架构中抽取视频图像信息数据库系统模型包含了视频图像信息数据库系统的内置服务功能。所有服务功能都要从接口功能中去体现。本模型具体规定了以下四个服务接口:

(1) 视频图像信息实时采集接口(简称 A 接口) :是视频图像信息采集系统与视频图像信息数据库之间的服务接口,主要是将采集的视频图像信息实时写入视频图像信息数据库。

(2) 视频图像信息应用服务接口(简称 B 接口) :是视频图像信息数据库系统与视频图像信息应用平台之间的服务接口,是将视频图像信息数据库系统功能以服务的方式开放给上层本地应用程序,包括独立的视频图像信息实战应用平台、各警种的业务系统等。值机人员在视频巡逻过程中通过视频监控联网共享平台采集的视频图像信息和侦查人员在侦查与研判过程中所采集与形成的视频图像信息均通过该接口存入视频图像信息数据库。

(3) 视频图像信息批量数据交换接口（简称 C 接口）：是视频图像信息数据库系统与公安信息化系统之间的批量数据交换接口。如交警对于违章车辆信息入库后需要进行人工核对,经过人工核对后的包括车牌在内的过车记录信息是准确的,如果将这部分经过人工核对的过车记录信息批量交换到视频图像信息数据库中,对相对应的过车记录信息进行更新,可以提高视频图像信息数据库的数据质量,另外也可实现案件受理登记信息的实时批量导入。

(4) 视频图像信息联网共享服务接口（简称 D 接口）：是上下级视频图像信息数据库系统之间的联网共享服务接口,实现视频图像信息数据库跨区域的共享应用。

7.2.5 大数据处理平台

7.2.5.1 大数据处理平台

（1） 架构设计

SDCHadoop 大数据基础平台集工作台、工作流开发环境、任务调度、数据管理、数据检索、集群运维管理系统和应用门户为一体,为用户提供基于大数据的基础解决方案,全面满足不同行业、不同人群对大数据的个性化要求。

运维管理（SDC Console）：SDC Console 是大数据运维管理系统,为 SDCHadoop 供高可靠、安全、容错、易用的集群管理能力,支持大规模集群的安装部署、监控、告警、用户管理、权限管理、审计、服务管理等。

SDC Hadoop 集成开发工具：提供了 web 图形化方式操作，包括流程控制、作业调度、数据管理、数据搜索、元数据管理、文件管理等功能。

HDFS:Hadoop 分布式文件系统（HadoopDistributed FileSystem），提供高吞吐量的数据访问,适合大规模数据集方面的应用。

Zookeeper ：提供分布式、高可用性的协调服务能力。帮助系统避免单点故障,从而建立可靠的应用程序。

HBase：提供海量数据存储功能,是一种构建在 HDFS 之上的分布式、面向列的存储系统。

Elasticsearch ：提供了一个分布式多用户能力的全文搜索引擎。

Parquet ：面向分析型业务的列式存储格式。

YARN 资源管理系统,它是一个通用的资源模块,可以为各类应用程序进行资源管理和调度。

Tachyon：

分布式内存文件系统,可以在集群里以访问内存的速度来访问存在 tachyon 里的文件。

Redis ：提供基于内存的高性能分布式 K-V 缓存系统。

MapReduce:提供快速并行处理大量数据的能力,是一种分布式数据处理模式和执行环境。

Spark：基于内存进行计算的分布式计算框架。

Strom：提供分布式、高容错的实时计算系统。

Hive ：建立在 Hadoop 基础上的开源的数据仓库,提供类似 SQL 的 Hive Query Language 语言操作结构化数据存储服务和基本的数据分析服务。

Impala ：提供 SQL 语义,能查询存储在 Hadoop 的 HDFS 和 HBase 中的 PB 级大数据。

Spark Streaming ：建立在 Spark 上的实时计算框架,通过它提供的丰富的 API、基于内存的高速执行引擎,用户可以结合流式、批处理和交互试查询应用。

Kylin ：支持在超大数据集上进行秒级别的 SQL 及 OLAP 查询。

（2） 功能模块

大数据运维管理

大数据运维管理为大数据存储供高可靠、安全、容错、易用的集群管理能力,支持大规模集群的安装部署、统一监控告警、统一用户权限管理、日志查询、服务管理等。

服务管理

提供服务管理,支持对各项资源及服务进行创建、删除、启停、重启、配置、升级、部署、维护等操作：

统一监控告警

提供集群监控功能,集成大数据服务、可视化服务、数据挖掘服务等,并对服务器 CPU、服务资源、服务状态（警告、错误、隐患） 进行实时监控,并以图表形式呈现。支持异常邮件报警，便于用户及时发现问题并处理：

日志查询

提供日志分析友好的 Web 界面,可以帮助用户汇总、分析和搜索重要数据日志：

统一用户权限管理

提供统一用户权限管理,方便管理员对用户进行管理：

SDC Hadoop 集成开发工具

提供了 web 图形化方式操作,包括流程控制、作业调度、数据管理、数据搜索、元数据管理、文件管理等功能。

流程控制

工作流是由多个节点和节点间的依赖关系所组成的一组逻辑和规则,形成一张有向无环图（DAG 图） 开发者可通过开发面板和管理面板新建工作流来新建工作流进入工作流设计器,在工作流设计器中通过拖拽不同类型节点并连线的方式来开发一个工作流,提供基本的数据集成、数据计算、数据调度等组件的工作流设计,支持工作流的新增、删除、修改、查询、测试运行、格式化、提交、保存。支持设置工作流任务定时执行,并实时监控任务执行情况,支持运行日志查看。

实时概况

采用多视图实时对流程运行进行监控,从状态、时段、步骤类型、耗时等不同角度查看过去 12 小时或 24 小时内所有流程的运行统计概况,帮助用户第一时间获知全局运行情况,并提供强大的性

能分析报告优化流程调度：

流程设计：通过简单的拖拽方式即可完成数据特征提取,样本数据建立,数据挖掘场景构建等复杂流程设计,界面简洁,操作简单：

工作流列表和工作流设计在同一页面,方便用户快速的切换工作流进行操作,提供工作流新增、删除、修改、查询、运行、保存功能：

提供工作流组件参数配置,满足用户各类流程设计需求：

用户可设置工作流调度,让流程任务定时执行：

提供工作流运行、暂停功能,运行过程中实时返回各步骤运行结果：

运行监控：展示进行中和已完成的工作流信息,信息主要包含流程名称、状态、提交者、启动时间、结束时间、运行进度：

提供关键词搜索流程功能,支持按状态和周期筛选工作流，方便用户快速查找：

提供运行中的工作流暂停、终止功能； 提供已完成的工作流再次运行、查看运行日志功能：

作业调度

通过多时间维度的计算任务调度、在线运维、监控报警等功能为大数据开发提供稳定的计算调度能力,可以支持超过百万级的调度任务量。

数据管理

支持关系型数据、Hadoop 等多种方式的数据查询操作。可指定数据库进行查询,支持历史查询记录查看：

提供图表化的查询结果展示,支持条状图、折线图、圆形图、映射图； 图表还可按升序、降序及正常序显示查询结果：

支持查询结果导出为 XLS 和 CSV 格式,还可保存到 HDFS 或者 Hive 中：

数据搜索

通过平台建立多维索引,实现分布式实时搜索与分析引擎,

可实时对数据进行深度搜索：

元数据管理

对元数据进行管理和操作,查看表结构、表的存储位置及样本数据。支持从文件创建一个表、手动创建一个表以及 Hadoop 体系与传统关系型数据库之间大批量数据的传输。

查看元数据信息,如表结构、样例数据及存储位置等,支持指定数据库查看：

支持手动创建一个表,后续数据导入到该表文件夹下,可实现对数据的查询等操作； 同时也支持从数据文件中导入数据的方式创建一个表：

文件管理

文件管理主要功能是实现对 Hadoop 文件的管理,实现海量数据文件的分布式存储。支持对文件进行新增、删除、修改、查询、权限更改等操作。支持查看历史记录以及从回收站恢复删除的文件.

分布式文件系统 HDFS

HDFS 是 Hadoop 的分布式文件系统,实现高吞吐量的数据访问,适合大规模数据集方面的应用,

为海量数据提供存储。

HDFS 包含主、备 NameNode 和多个 DataNode。在 HDFS 内部，一个文件分成一个或多个 “数据块” DataNode 集合里,NameNode 负责保存和管理所有的 HDFS 元数据。客户端连接到 NameNod，执行文件系统的“命名空间” 操作,例如打开、关闭、重命名文件和目录,同时决定“数据块” 到具体 DataNode 节点的映射。

DataNode 在 NameNode 的指挥下进行“数据块” 的创建、删除和复制。客户端连接到 DataNode,执行读写数据块操作。

分布式批处理引擎 MapReduce

MapReduce 是用于并行处理大数据集的软件框架。MapReduce 的根源是函数性编程中的 map 和 reduce 函数。Map 函数接受一组数据并将其转换为一个键/值对列表,输入域中的每个元素对应一个键/值对。Reduce 函数接受 Map 函数生成的列表,然后根据它们的键缩小键/值对列表。MapReduce 起到了将大事务分散到不同设备处理的能力,这样原本必须用单台较强服务器才能运行的任务,在分布式环境下也能完成了。

统一资源管理和调度框架 YARN

YARN 是 Hadoop2.0 中的资源管理系统,它是一个通用的资源管理模块,可以为各类应用程序进行资源管理和调度。YARN 不仅局限于 MapReduce 一种框架使用,也可以供其他框架使用,比如 Tez、Spark、Storm 等。YARN 主要分为 ResourceManager、ApplicationMaster 与 NodeManager 三个部分。

ResourceManager：RM 是一个全局的资源管理器,负责整个系统的资源管理和分配。它主要由两个组件构成：调度器（Scheduler ） 和应用程序管理器 （Applications Manager） 。

调度器根据容量、队列等限制条件(如每个队列分配一定的资源,最多执行一定数量的作业等），将系统中的资源分配给各个正在运行的应用程序。调度器仅根据各个应用程序的资源需求进行资源分配,而资源分配单位用一个抽象概念 Container 表示。Container 是一个动态资源分配单位,它将内存、CPU、磁盘、网络等资源封装在一起,从而限定每个任务使用的资源量。

此外,该调度器是一个可插拔的组件,用户可根据自己的需要设计新的调度器,YARN 提供了多种直接可用的调度器,比如 FairScheduler 和 Capacity Scheduler 等。

应用程序管理器负责管理整个系统中所有应用程序,包括应用程序提交、与调度器协商资源以启动 ApplicationMaster 、监控 ApplicationMaster 运行状态并在失败时重新启动它等。

NodeManage：NM 是每个节点上的资源和任务管理器。一方面,它会定时向 RM 汇报本节点上的资源使用情况和各个 Container 的运行状态； 另一方面,它接收并处理来 AM 的 Container 启动/停止等各种请求。

ApplicationMaster ：AM 负责一个 Application 生命周期内的所有工作。包括：

与 RM 调度器协商以获取资源。将得到的资源进一步分配给内部的任务 (资源的二次分配）。

与 NM 通信以启动/停止任务。

监控所有任务运行状态,并在任务运行失败时重新为任务申请资源以重启任务。

分布式数据库 HBase

HBase 是一个高可靠性、高性能、面向列、可伸缩的分布式存储系统。HBase 适合于存储大表数据（表的规模可以达到数十亿行以及数百万列） 访问可以达到实时级别。HBase 集群由主备 Master 进程和多个 RegionServer 进程组成：

利用 Hadoop HDFS（Hadoop Distributed File System ）作为其文件存储系统,提供高可靠性、高性能、列存储、可伸缩、实时读写的数据库系统。

为 Spark 和 Hadoop MapReduce 提供海量数据实时处理能力。

利用 ZooKeeper 作为协同服务。

分布式内存计算框架 Spark

Spark 是一个并行数据处理框架,能够帮助用户简单的开发快速,统一的大数据应用,对数据进行,协处理,流式处理,交互式分析等等。

Spark 具有如下特点：

快速：数据处理能力,比 MapReduce 快 1 0-1 00 倍。易用：可以通过 Java,Scala ,Python ,简单快速的编写并行的应用处理大数据量,Spark 提供了超过 80 种高层的操作符来帮助用户组件并行程序。

普遍性：Spark 提供了众多高层的工具,例如 Spark SQL，MLib,GraphX,Spark Stream ,可以在一个应用中,方便的将这些工具进行组合。

与 Hadoop 集成：Spark 能够直接运行于 Hadoop 2.0 的集群,并且能够直接读取现存的 Hadoop 数据。尤其，Spark 和 Hadoop 密结合,可以通过大数据基础平台 Console 部署安装 Spark。

Spark Streaming 是一种构建在 Spark 上的实时计算框架，它扩展了 Spark 处理大规模流式数据的能力。

Spark SQL 是 Spark 中用于结构化数据处理的模块。Spark SQL 提供了一种通用的访问多数据源的方式,可访问的数据源包括 Hive、Avro、Parquet、ORC、JSON 和 JDBC 数据源,这些不同的数据源直接也可以实现互相操作。Spark SQL 复用了 Hive 的前端处理逻辑和元数据处理模块,使用 Spark SQL 可以直接对已有的 Hive 数据进行查询。另外,SparkSQL 还提供了诸如 API、CLI 、JDBC 等诸多接口,对客户端提供多样接入形式。

分布式搜索 ElasticSearch

ElasticSearch 是一个实时分布式搜索和分析引擎：

可用于全文搜索、结构化搜索、文本分析；

提供了一个分布式多用户能力的全文搜索引擎,基于 RESTful web 接口,目的是通过简单的 RESTful API 来隐藏 Lucene 的复杂性,从而让全文搜索变得简单；

使用 Java 开发的,用于复杂应用底层的搜索功能开发。

Elasticsearch 不仅仅是 Lucene 和全文搜索,还支持以下特性：

分布式的实时文件存储,每个字段都被索引并可被搜索；

分布式的实时分析搜索引擎；

可以扩展到上百台服务器,处理 PB 级结构化或非结构化数据。

Elasticsearch 是面向文档 (document oriented) 的：

可以存储整个对象或文档 (document) 。

同时会索引 (index) 每个文档的内容使之可以被搜索。

在 Elasticsearch 中,可以对文档（而非成行成列的数据）进行索引、搜索、排序、过滤。

数据仓库 Hive

Hive 是建立在 Hadoop 上的数据仓库框架,提供类似 SQL 的 Hive Query Language 语言操作结构化数据,其基本原理是将 HQL 语言自动转换成 MapReduce 任务或 Spark 任务,从而完成对

Hadoop 集群中存储的海量数据进行查询和分析。Hive 主要特点如下：

海量结构化数据分析汇总；

将复杂的 MapReduce 编写任务简化为 SQL 语句。

灵活的数据存储格式,支持 JSON,CSV,TEXTFILE,RCFILE, SEQUENCEFIL, EORC（Optimized Row Columnar ） 这几种存储格式。中的元数据包括表的名字,表的列和分区及其属性,表的属性（是否为外部表等） 录等。

Hive 为单实例的服务进程,提供服务的原理是将 HQL 编译解析成相应的 MapReduce 或者 HDFS 任务：

流处理 Storm、Spark Streaming

Apache Storm 是一个分布式、可靠、容错的实时流式数据处理的系统。在 Storm 中,先要设计一个用于实时计算的图状结构,我们称之为拓扑（topology ） 被提交给集群,由集群中的主控节点（master node ） 分发代码,将任务分配给工作节点（worker node） 执行。一个拓扑中包括 spout 和 bolt 两种角色，其中 spout 发送消息,负责将数据流以 tuple 元组的形式发送出去； 而 bolt 则负责转换这些数据流,在 bolt 中可以完成计算、过滤等操作,bolt 自身也可以随机将数据发送给其他 bolt 。由 spout 发射出的 tuple 是不可变数组,对应着固定的键值对。

Spark Streaming 是一种构建在 Spark 上的实时计算框架，它扩展了 Spark 处理大规模流式数据的能力。Spark Streaming 具备以下特性：

能运行在 1 OO+的结点上,并达到秒级延迟。

使用基于内存的 Spark 作为执行引擎,具有高效和容错的特性。

能集成 Spark 的批处理和交互查询。

为实现复杂的算法提供和批处理类似的简单接口。

分布式缓存层（Tachyon、Redis ）

Tachyon 是 Spark 生态系统内快速崛起的一个新项目。本质上,Tachyon 是个分布式的内存文件系统,它在减轻 Spark 内存压力的同时,也赋予了 Spark 内存快速大量数据读写的能力。

Tachyon 把内存存储的功能从 Spark 中分离出来,使 Spark 可以更专注计算的本身,以求通过更细的分工达到更高的执行效率。

Tachyon 可以有效地解决如下问题：当两个 Spark 作业需要共享数据时,无需再通过写磁盘,

而是借助 Tachyon 进行内存读写，从而提高计算效率。在使用 Tachyon 对数据进行缓存后,即便在 Spark 程序崩溃 JVM 进程退出后,所缓存数据也不会丢失。这样，Spark 工作重启时可以直接从 Tachyon 内存读取数据了。当两个 Spark 作业需要操作相同的数据时,它们可以直接从 Tachyon 获取,并不需要各自缓存一份数据,从而降低 JVM 内存压力,减少垃圾收集发生的频率。

Redis （REmote DIctionary Service ） 支持多种数据类型，集群扩容、减容,Balance 。

数据类型：包括 string （字符串）、list （表）、set （集合）、zset （有序集合）、hash 等。

集群扩容、减容：当集群需要提供大规模的处理能力时，可以一键式扩容一对或多对主从实例。在此过程中,系统会自动完成数据迁移和数据平衡,用户无需其他操作。

Balance ：出现扩容异常、部分实例掉线等异常场景时，Redis 集群中的数据可能会分布不均匀,此时可以通过管理界面上提供的 Balance 功能,让系统自动对集群数据进行平衡,保证集群的健康运行。

分布式应用程序协调服务 ZooKeeper

ZooKeeper 是一个分布式、高可用性的协调服务。主要支持以下特性：

帮助系统避免单点故障,建立可靠的应用程序。

提供分布式协作服务和维护配置信息。

ZooKeeper 集群中的节点分为三种角色：Leader、Follower 和 Observer ,其结构和相互关系。通常来说,需要在集群中配置奇数个（2N+1） ZooKeeper 服务,至少（N+1） 个投票才能成功的执行写操作。

（3） 功能特性

安全性加固

SDC Hadoop 大数据基础平台通过架构安全、认证安全、文件系统层加密实现多维度安全管理。架构安全基于微服务架构方式,针对每个微服务请求之间保持服务的相互认证； 用户认证安全基于用户和角色的认证体系,支持安全协议 Kerberos ,使用 LDAP 作为账户管理系统,提供单点登录能力；文件系统层针对表、字段的存储关键信息动态加密,集群内部用户信息禁止明文存储。

统一工作台

SDC Hadoop 统一工作台提供丰富的可视化组件,包括批量采集、实时采集、实时消息、批量计算任务、机器学习等任务类 型。

提供自动化的二次开发助手和开发样例,帮助软件开发人员快速上手。相较于开源的工作流拖拽,提供更为便捷和灵活的体验与交互。

资源动态管理

SDC Hadoop 大数据基础平台在统一存储上建立资源管理层，提供企业用户统一的计算资源管理、动态资源分配、多租户之间资源配置和动态共享,灵活支持多租户多服务在统一平台上平滑运行； 在可管理性方面优势显著； 大数据基础平台基于 YARN，支持同时运行多个计算框架。

统一运维管理

SDC Hadoop 大数据基础平台作为企业级解决方案,开发了用户友好的图形化管理界面、提供了

系统安装、集群配置,资源 级别安全控制、监控及预警等多方面支持,在可管理性方面优势显著;

全 路大数据管理

SDC Hadoop 大数据基础平台提供个性化的数据建模、数据查询、收藏、管理功能,用户可轻松收藏所关注的数据表,同时可对数据表的生命周期、基本信息、负责人等信息进行管理,也可查看数据表存储信息、分区信息、产出信息、血缘信息等内容。

海量批处理和高速流处理

SDC Hadoop 大数据基础平台基于 Labmda 架构,有机集成了 Hadoop、Spark、Storm 等计算框架和 HDFS、Hbase 等数据存储服务,真正做到海量批处理和高速流处理的能力。

海量数据搜索

SDC Hadoop 大数据基础平台分布式实时搜索与分析引擎，可实时对数据进行深度搜索,支持多维度的数据展现形态。

7.2.5.2 大数据多维分析查询系统

（1） 架构设计

（2） 功能模块

多数据源管理

支持多种数据源的连接,包括：主流关系型数据库 RDBM、S

Excel/CVS 文本数据源、基于 hadoop 的大数据平台数据源以及

其他多种 JDBC 数据源。

数据建模

数据源建好之后,支持对数据表进行进行数据建模,构建 BI 分析需要的维度、指标。大数据多维分析查询系统支持星型、雪花模型,拖拽式可视化建模。模型创建后,系统自动生成 Cube,供 BI 分析使用。

平台智能识别出维度和指标信息,并且支持对维度、指标的转换。

工程化管理

支持工程模式的管理,一个工程下支持多个页面,也支持多个分组,分组下还可以新建页面,便于对多个可视化页面进行分类管理。工程发布后,工程名字即是发布报表的一级菜单,里边的分组是二级菜单。

支持对工程的新增、删除、发布、复制、导入、导出功能。

可视化编排

SDC UE 大数据多维分析查询系统是基于 JS 代码开发的 IDE,可以在各种浏览器下实现报表制作。通过所见即所得拖拽方式实现灵活的可视化布局,极致的用户体验。您只需要通过拖拽,无需编程能力,在设计器上任意发挥创意,即可创造出专业的 BI 报表和可视化数据展现 Web 页面。

支持字体对齐,组件对齐,组件分布,组件层级控制等等， 相关操作非常便利：

字体对齐支持：文本左对齐、文本居中对齐、文本右对齐。

组件对齐支持：左对齐,左右居中,右对齐,顶端对齐,上下居中,低端对齐。

支持组件横向自动分布,组件纵向自动分布。

画布上支持标尺,提供标尺对齐线。

提供坐标显示、设置,长度、宽度直接设置。

支持画布大小选择,自定义社会。

支持拷贝、粘贴、上下左右移、回退、重做、保存、全部保存等快捷键。

当组件重叠的时候,支持设置组件层级,可以置顶或者降底。样式支持对不同的组件,包括基础组件、图标组件、GIS 组件等设置不同的样式,以满足不同的需求场景。

为了提高开发效率,为开发者提供了自定义布局模板和业务模板的保存。方便后续的项目可以承之前项目的一些成果进行复用。布局模板只 承页面设置框架。业务模板在布局模板的基础上集成了和业务相关的数据模型的绑定。

可以将饼图和一个混合图配置好之后,把他们一起保存为自定义业务组件,保存到平台中。下次相同的业务场景,就可以直接将这个自定义业务组件 “饼图 +混合图组合组件” 拖到页面中,不需要再重新配置。

组件库

系统既支持柱状图、折线图、饼图、雷达图、散点图、玫瑰图、气泡图、矢量地图等多种基本图表,同时支持漏斗图、词云图、GIS 地图等特殊图表,满足不同场景的数据展现需求。特别是系统支持丰富多样的 WEB 组件。

图表组件

当前支持的有：面积图、条形图、趋势图、混合图、饼图、折线图、柱状图、折线堆积图、柱状堆积图、面积堆积图、表格、条形堆积图、南丁格尔玫瑰图、嵌套饼图、仪表盘、大规模散点图、标准气泡图、漏斗图、雷达图等等,样式丰富 ， 且支持自定义扩展。

图标组件及相关功能介绍如下：

表格组件

SDCUE 大数据多维分析查询系统具备灵活额表格组件,实现对详细数据的表格化呈现。

表格的能力支持：每页行数控制、加载上限、滚动高度设置、单元格冻结、复选框、行序号、分页、搜索、多了排序、表头设置、数据区设置、背景及背景图片设置、奇偶行设置、边框设置、网格线设置,同时支持动态筛选、动态列选择、动态排序、异步加载、表格渲染、数据导出等动作。

地图组件

GIS 地图

GIS 组件支持用户自定义图层,提供多种控件和渲染方式， 支持两种底图,支持卫星图。将带有 “地域性” 或“区域性” 特征的信息通过地图的形式进行展现,更加直观地监控每个地区的业务情况。

矢量迁移地图

支持迁移、流向场景的质量地图。用于直观地体现各种数据在省（直辖市）、市（州） 的流动。

矢量分布地图

支持全国、省（直辖市）、地市（州） ,三级分布地图。让用户非常直观地监控不同地区的业务发展和绩效情况。地图区域采用不同颜色进行显示、或在地图区域上放置不同颜色的旗帜,决策层可以清楚了解企业的战略执行,并通过在地图上实现下钻操作及联动图形,探索问题的根源,增强洞察力。

多维 BI 分析

SDC UE 大数据多维分析查询系统提供了各种常见的 OLAP 分析操作,除基本的分组聚合外,还可以进任意多维度分析,包含：钻取、切片、切块、旋转、排序、过滤等分析功能。

拖拽式自由分析

在多维 BI 分析一体化工作台中,您可以选择任意数据模型中的任意维度、度量进行自主拖拽分析。同一个模型中,所有的数据已经关联在一起了,这就决定了多维及时分析的自由度。同时，在一个页面就能进行数据模型选择、维度指标选择、图表选择、图表样式设置、数据预览。

多层钻取

在进行 BI 分析时,支持自由创建维度间的层级关系,构建维度分级。将具备层级的维度应用到各种图表上,即可实现自动多层钻取能力,逐层分析和查看各种数值情况。下钻之后,还能自由地返回上级。

组合过滤

提供以条件过滤的方式进行多维切片、切块分析。条件过滤可以应用到任意一个维度,即使该维度没有被用在图表上进行分析,增加了过滤的宽泛和强大性。过滤条件支持：大于、小于、大于等于、小于等于、包含、不包含、不等于、等于等各种条件判断,同时,每个条件判断支持采用逻辑表达式的方式组合,形成强大的过滤模型,满足各种切片和切块需要。

聚合

在数据分析工作中,除了对普通数据的维度、度量进行直接分析和观察数据的整体效应外,分析平均数、最大值、最小值、分位数等需求也是常见的。如果汇总方式仅有单一的求和汇总，则很难满足这类需求。

在 SDCUE 大数据多维分析查询系统中,能进行数据动态呈现的所有表格、图表、基本 WEB 组件除可进行分组或交叉汇总外，可以针对以选择的任意度量进行求和、求最值、求平均、求分位数等,并且它们之间可以实时切换。

自定义计算度量

度量（指标） 可以来自于原始的数据字段,同时也可以是通过公式计算得来。

SDCUE 支持创建自定义计算字段。这些新增字段是通过原有的一个或者多个数据字段,采用几十种普通的数学公式函数计算而来。比如：有一个垃圾短信字段、一个正常短信字段,那么在原本没有总发送短信字段的时候,就可以通过这两个字段相加而得到。

数据格式转换

针对度量数据,支持在分析时对这些数据进行格式转换,包含：时间转换、浮点数转换、流量转换、百分比转换、单位转换、经纬度转换、枚举值转换、服务区时间转换等等,还可以采用 JavaScript 代码,自定义转换函数。

数据格式转换及自定义代码

页面级编排

SDC UE 大数据多维分析查询系统不仅仅能进行 BI 分析,编排通用的 Dashboard 报表页面,也能基于丰富的 WEB 组件,像 Dreamweaver 一样设计出用于数据呈现、数据查询、数据联动、数据分析的全套 WEB 系统。

相比于普通可视化分析产品只能编排出全图表式的 Dashboard 页面,SDCUE 编排出的 WEB 页面支持丰富的 WEB 组件，以进行数据查询、图表之间联动、页面间联动和参数传递。

WEB 表单组件

为了在进行 BI 分析的同时,也能编排出一个完整的数据呈现 WEB 系统。SDC UE 增加了独有的 WEB 表单组件。通过这些组件，可以设计出多样化的,具备交互能力的 WEB 系统。使得 BI 分析和页面展现一体化。

当前支持的有：文字控件、文本编辑、按钮、下拉框、单选框、复选框、上传组件、时间组件、矩形组件、开关组件、超接组件、树组件、表单容器、Tab 容器、查询容器、图片、菜单、行布局、状态设置、列布局、iframe 容器、胶片容器、线条等等,样式丰富,且支持自定义扩展。

部分 WEB 组件的功能介绍如下：

动态查询

丰富灵活的查询条件,支持运行时动态查询。

通过丰富的查询手段,既能满足普通用户自助式的简易查询需求,又能满足数据分析师的专业需要。业务用户可以轻松的访问、浏览和探察数据； 满足业务人员自助式的、零编程的、快速的定制查询,数据分析。

事件可编程

可以为大多数组件设置事件动作的响应,包含：左键单击、左键双击、鼠标进入控件、鼠标划过控件、鼠标离开控件、控件初始化完成、控件渲染完成等等。

联动设置：多表可配置进行维度、度量关联分析,帮助用户深入了解数据关系。支持多表联动,单向联动,多向联动。联动操作触发的控制条件：

可以选择多种动作类型,包含：联动、跳转、服务调用、弹出窗口、关闭窗口、自定义动作。

事件触发后的组件动作：

跳转设置：可以通过跳转功能,来实现钻入和钻出的效果,跳转到预先设置好的不同维度的页面,查看下级数据。同理也可在钻入后的页面设置跳转动作到原页面,实现钻出效果。在钻入钻出的同时,支持带入参数值,并且可以自定义写入代码来实现相关效果。

调用接口设置：当组件所对应的的事件动作类型为服务调用时,可以设置服务访问类型为 API

接口。当点击 URL 之后,可以选择预先定义好的接口来进行触发相应的处理,如查询数据,事务处理流程等等。

接口选择页面,支持检索和分页:

弹窗设置:当组件所对应的的事件动作类型为弹出窗口时,可以设置弹窗内容,以及通过参数设置,可以控制弹出窗口的样式如标题,背景色,遮罩等等。

JavaScript 开发接口:当需要配置的参数格式不满足项目要求时,开发者也可以通过 Json 代码自定义参数,通过代码转换成自定义参数。

实时分析/计算引擎

独有的实时分析/实时计算引 擎将会帮助 SDC UE 相比传统的 BI 系统得到十倍以上的提升。针对 TB 级、PB 级的数据量的所有分析请求能根据不同请求对象自动进行负载均衡,保障结果能在一秒之内返回结果。这一架构的好处及技术显而易见的:

尽量发挥机器系统的特点,避免远程访问数据库,加快数据的计算;

精心设计的存储结构以利于高速运算;

特有的跨粒度计算、内存计算、流计算、库内计算、列存储、并行计算等技术来加速数据的计算;

避免频繁的 IO 访问和远程访问数据库。

得益于 SDCUE 大数据多维分析查询系统跨粒度计算,所有的计算都会被以最优化的方案转化为库内计算,从而获取最好的性能。各种常见的汇总函数,以及几乎所有的统计函数都支持。为了更好的理解数据,我们提供了自定义模型能力,可将以形成业务模型进行引用。

我的报表

发布与授权

SDC UE 大数据多维分析查询系统的页面支持按照工程级发布,在发布时,可以对这个工程及所有页面进行授权管理,确定能被哪些用户查看。

报表查看人员可以在“我的报表” 查看在自己权限内的所有报表工程以及相关页面。报表发布页面以缩略图的方式只管呈现。

导出

每个 Dashboard 报表支持多种方式的导出,包括:

针对单个图表,支持以图片的方式直接导出到本地;

支持将页面编排效果导出为 PDF 格式的文件。

引用

SDCUE 大数据多维分析查询系统发布的报表工程、页面,能通过 URL 或者 API 接口方式嵌入到第三方应用系统。根据安全要求以及第三方系统特性,同时支持免登陆方式和权限认证方式。

集成与安全

基础管理

提供完整的基础管理系统,包含:地区管理、部门管理、人员管理、安全管理、日志管理、系统

设置等。提供统一的登录认证门户。

安全管理

提供用户、角色、权限三级管理机制。通过用户管理控制进行按照部门、地区、不同角色、不同用户进行精细化授权。

对于 URL 的访问安全,同时支持免登陆模式和认证模式。对于免登陆模式,可以直接打开 URL 页面。对于一些需要进行权限保护的 URL 页面,系统提供统一的权限管理机制,所有试图打开 SDC UE 大数据多维分析查询系统所发布的页面 URL 的第三方系统,都需要申请和登记,系统会为这些系统分配唯一标志,只有符合条件的系统才能够调用 SDC UE 大数据多维分析查询系统的报表页面。因此,就算外部系统或者其他人员拿到了这些 URL 页面地址,也无法访问。

对于数据安全,在报表配置页面,针对每一个维度、指标，都可以进行脱敏处理,包含：对数据加密显示或者屏蔽显示。

部署与集成

SDCUE 大数据多维分析查询系统能够非常方便的与其他应用进行集成。提供专门的 SDK 组件、丰富的二次开发调用接口,配以深入浅出的帮助和样例文档,让开发者很容易就能上手。

在平台集成和客户化功能方面,大数据多维分析查询系统开发的报表是完全基于 HTML5 技术,可以灵活和第三方进行集成应用和跨平台部署。

平台支持基于 CAS 认证的标准 SSO 单点登录技术和接口,可以很轻松地集成其他业务系统,同时也能被集成到第三方业务系统（要求提供标准的 SSO 接口） 中去。

国际化

SDC UE 大数据多维分析查询系统支持中文、英文双语版本，支持双语实时切换,面向全球的客户使用。无需单独购买版本。

（3） 功能特性

极致的用户体验

安装和维护成本低

支持一键式自动部署

无需技术背景,业务人员即可操作

只需部署一次,使用人员无需单独安装,随时随地办公，只需要一个浏览器即可

丰富简单的数据建模主流关系型数据库（RDBM）SExcel/CVS 文本数据源

基于类 hadoop 的大数据平台、数据仓库、数据集市其他 JDBS/ODBC 数据源灵活数据建模功能,让零基础用户轻松驾驭多源数据自由式轻松编排

全拖拽式图形化编排,只需要动动鼠标自由布局,自动排版多种样式主题,一键切换,一键整体换肤,无需单个配色多种排版工具栏、快捷操作,具备 Microsoft PPT 一样的编排体验惊艳的组件

多达 50 个以上的图表组件

支持 3D 图表

支持 GIS 地图组件

支持矢量地图（分布图、迁移图等）

多维度智能分析

支持多维分析：多层钻取、切片/切块、旋转、排序

支持并行计算,内存计算,秒级刷新

支持动态绘制、动态刷新、动态维度切换简单而又有深度

以用户为本,支持多用户类型

具备面向业务人员的傻瓜相机式使用,也支持专业人员的单方相机式使用

支持一键式、傻瓜式、自动式编排和分析

全称无需编码也能轻松设计输出报表

支持复杂的 WEB 系统级设计

支持复杂多样的组件事件配置、事件响应动作、参数传递

支持采用 Javascript、JSON 等脚本语言进行自定义编程安全可依赖

提供地区、部门管理,支持集团式、分区式用户权限管理提供用户、角色、权限三级管理

URL 集成具备免登陆式和权限认证式

支持数据级别访问安全控制

7.2.5.3 大数据智能分析系统

（1） 架构设计

SDC Miner 大数据智能分析系统是以数学模型训练从创建，到模型管理应用,全生命周期为核心的体系化建设方案,并在此基础上,拓展多样化的数据输入、导入接口,并建立基于客户账户个性化应用的算法管理体系,并辅以基础管理功能提供整体管理功能。从而实现客户多样化体系化的算法模型应用需求。

（2） 功能模块

大数据挖掘是一项系统性的工程,其涉及到数据探索、数据处理、模型建立、模型训练等一系列过程。因此,单一的步骤不足以表示大数据挖掘的全过程。SDC Miner 大数据智能分析系统使用建模的概念来表示整个过程。其主要建模流程及功能如下所述：

数据源

关联数据是建模的第一步,用户可以在数据源直接连接数据库或导入本地数据,并可通过新建文件夹或保存到相关的文件夹的方式来对数据进行方便有效的管理。

支持多种数据库类型

基于大数据的 HIVE、HDFS 等;

传统关系型数据库 Oracle、Mysql、DB2、PostgreSQL 等。

支持多种格式的本地数据

本地数据支持类型：excel、txt、csv 等。

模型训练

建模过程是一个不断尝试不断探索的过程。用户从原始数据出发,经过对数据的探索和处理,运用合适的算法,最终形成业务上可用的模型。

易用性模型搭建

在 SDC Miner 大数据智能分析系统中,每一个流程都是由多个算法组成,复制一个算法的同时也复制了其参数配置,极大的方便了用户快速构建大规模数据挖掘系统。每个算法接受若干输

入,产生若干输出。每个算法的输出都可以作为其他算法的输入。用户只需把自身业务系统相关的算法拖拽到设计面板内,按需连接输入输出端,即可完成流程设计。

多类型算法支持

SDC Miner 大数据智能分析系统内置

流程多分支设计

在建模的过程中,会有很多尝试性的步骤,用户还可以通过在流程设计中添加算法分支的方式来对比进行不同的尝试方法， 然后根据预测结果找到最佳的预测算法,帮助客户产生更多价值。

流程管理

在流程设计过程中,用户可以随时保存操作步骤,下次打开该流程时 续进行设计。

当流程设计完毕后,用户可以保存设计步骤,这样就可以在同类型条件下使用该流程来输出模型结果,大大缩减了流程重设计的时间。流程只记录了原始数据如何一步一步转换为最终模型结果的过程,所不同的是,该流程只保留了输出模型结果的必要步骤,不再保留用户在建模时所做的尝试性工作。

可视化结果

建模的目的就是将读取的数据通过一系列算法组合得到最终的模型结果。然后通过数据统计和分析图表等可视化的方式展示,供用户更直观的从图表中发掘数据背后的意义。

实时监控

在模型搭建或运行期间,用户可随时查看每个算法的运行状态、运行结果和时间。还可查看其运行日志,便于用户排查运行故障。

自定义算法

SDC Miner 大数据智能分析系统从业务落地出发,帮助客户有效的管理大数据挖掘的各个阶段,不仅为客户内置了丰富多样的数据挖掘算法,同时也为用户提供了强大的自定义算法功能及其便捷的管理系统。

客户可根据自身业务需求上传算法 JAR 包,并可对自定义算法进行编辑、启用、停用和删除操作,以便于对算法进行管理。

编辑自定义算法：用户可根据业务实际需求,对自定义算法进行基本信息、端口信息、参数信息相应的配置；

启用自定义算法：启用某个自定义算法后,它将在算法库的相应分类下展示,便于用户设计流程时调用；

停用自定义算法：停用某个自定义算法后,它将在算法库的相应分类下删除,便于用户对算法库进行整理；

删除自定义算法：删除某个自定义算法后,它将在算法库和算法列表中同时删除（但不影响占用流程的运行），便于用户对自定义算法的管理。

（3） 功能特性

强大的预测模型

提供行业里最全面的系列建模技术

支持 GB 到 PB 级数据量训练

超大数据集

高吞吐量的数据读取

高可扩展性,轻松应对数据量持续增长高性能处理

高效的并行化处理方式流式的数据访问,一次写入多次读写高效的结构化、非结构化处理性能简洁的模型训练

无需编写代码,简单拖拽即可操作可快速创建、更新模型配置

流程多分支同时训练

支持流程多个分支同时训练

提供简洁易懂的可视化分析报告对比训练结果

丰富的数据挖掘算法

几十种数据挖掘算法

可覆盖各类业务分析需求

强大的扩展性

支持多种类数据源

可以支持 Excel、txt、csv 等本地数据

可连接 HIVE、HDFS、Oracle、Mysql、DB2、Postgresql 等数据库

可信赖的安全控制

提供用户管理及多种权限控制设置

支持数据级别访问安全控制

支持资源级别访问安全控制

7.2.6 数据管理服务平台

数据管理服务平台是一个管理、展现平台,主要包括：数据治理与监控系统、数据服务集成管理

系统和大数据展现门户等。

7.2.6.1 数据治理与监控系统

（1） 架构设计

SDC 数据治理与监控系统是对数据资产管理行使权力和控制的活动集合（规划、监控和执行）。数据治理职能指导其他数据管理职能如何执行。

大数据治理贯穿在数据管理的整个过程中,重点关注的是有关数据的战略、组织、制度等高层次的话题,并通过制定和推行战略、组织、制度,将其他几个数据管理职能贯穿、协同在一起，让数据治理工作能够成为一个有机的整体而不是各自为政。

数据治理与监控系统,作为数据平台的管控系统,从制度、标准、监控、流程结果方面提升数据信息管理能力,解决目前所面临的数据标准问题、数据质量问题、元数据管理问题。建立统一、规范并且唯一的数据标准来解决信息交互、集成、统计、决策等诸多难题,有效地提高检验管理过程控制和质量。

（2） 功能模块

1 ）治理准备

治理准备主要依托元数据完成数据标准的建立,实现从逻辑建模到物理建模的全过程管理。

治理准备功能模块不仅提供技术元数据,如建模设计、数据元、代码集,数据集等,还提供业务分类、段码管理等业务元数据。丰富、灵活的、规范的元数据管理为实现互联互通、信息共享、业务协同以及安全可靠提供必要前提。

a）数据元管理

数据元标准管理主要包括数据元管理、数据类目管理以及代码管理功能。数据元的表示规范遵循 GB/T 1 9488.1 -***4 。

数据元的类型支持中文字符,字母字符,数字字符,数值型，字母数字字符,日期型,时间性,二进制类型（用来表示图形，相片,图片之类的数字流）：

提供对数据元进行新增,修改,删除,导出,导入等功能；

支持分数据元类目对数据元进行管理和维护；

提供对数据元类目进行新增,修改,删除操作,用户可以根据自己需要自定义数据元类目,然后对数据元进行管理；

支持按照数据元名称、标记等不同维度对数据元进行查找,方便用户对数据元的定义、格式等关键信息进行了解。

b）代码集管理

用户可以通过代码集管理模块对所需要的所有代码集进行管理、维护,主要操作包括新增,修改,删除,导出,导入；

可通过代码名集名称、序号等信息对代码集及其代码进行查找,已查看代码集的取值范围。

c) 数据集管理

数据集,即数据的集合。主要用于对数据元分类管理,并建立数据项。

数据集管理主要包括：

支持代数据集管理操作：新增、修改、删除、查看、查询；

支持前段码的发布功能；

支持段码模板的下载和数据的导入导出功能。

d) 目录管理

采用目录服务技术,对数量多、分类广、分散在不同机构的信息资源特征进行描述； 通过对目录内容采用灵活的多级目录配置方式,根据使用者适合自己业务领域的信息资源目录查找关心的信息资源,并可对资源信息进行维护,形成机构之间信息资源物理分散、逻辑集中的信息共享模式,实现以目录树的形式展现标准信息,帮助用户查找定位目录内容。

若在上级目录系统或其他平台已有目录,在目录标准中需要创建时,只需配置好相关连接信息,通过 Webservice ,调用其他系统的信息到目 录标准管理进行自动编目 ,不需要进行二次创建和配置,节省使用者的配置时间,提高工作效率。

支持逐级对不同的目 录类型 （如主题目 录,资源形态目 录等）的目录进行新增、修改、删除等操作,并支持对目录进行编号以及对目录类型的增加、修改、删除等功能。

e) 段码管理

段码管理主要是对信息类的编码进行管理,它分为：前段码和后段码； 其中,前段码的分配需要办理人员向管理人员提出需求后,交由管理人员统一分配,避免信息重复。后段码为信息类进行审核并发布后,在后段码管理中对信息类的后段码信息进行查询。

前段码由 5 位数字组成,其中前 2 位主要区分不同的省、自治区等,第 3 位为省级目录管理者和政务部门,第 4 位为地市目录管理者和政务部门,第 5 位为区县目录管理者和政务部门,管理者通过选择所属地区和部门,自动生成相应的编码信息,如：29002,代表省发展改革委的编号,其中,290 为省级部门管理者编号,02 代表发展改革委的部门编号。

后段码由 7 位数字和字母组成,其中前 2 位主要区分不同的部门,由省级目录管理者分配编号,第 3 位为大写字母,标识信息类所属类型,由各部门定义,第 4 位为大写字母,标识信息类主体类型,第 5~7 位由数字组成,由顺序号 001 ~999 组成； 如：

10AB001,其中 1 0 表示部门为 XX 高新区经济技术开区,A 代表信息类所属业务类别为婚姻登记,B 表示信息类主体类型为自然人， 001 代表信息类的顺序号。

后段码是各部门的信息资源。

f) 建模设计

支持可视化拖拽方式,对多种类型的数据库进行物理建模；

用户可在 web 界面上进行表分类、表创建、表关系配置,支持从多元数据库中读取已有表,并配置表关系。

2) 治理过程

治理过程,以校验和跟踪各个业务系统数据质量问题、提供数据质量提升的有效解决方案,最终提高业务数据质量为目标。

通过项目建设,提高数据质量检查的有效性,为多个业务系统的数据质量保驾护航。

通过制定、实施数据质量检验,暴露各系统数据质量问题。

持续监控各系统数据质量波动情况及数据质量规则占比分析,定期生成各系统关键数据质量报告,掌握系统数据质量状况。结合系统提供的清洗组件以及数据质量问题处理流程为各系统数据质量提升提供有效支撑。

a) 质量规则

制定统一的数据质量校验体系,统一数据质量度量、数据质量逻辑处理、执行的规范化步骤,可提升整体数据质量。对不满足要求的数据,可快速分析出数据的问题并闭环处理。

数据质量校验规则是为源系统中存在的数据质量问题建立标准数据规范,从而得到有效的、可用的数据。

b) 任务调度

通过制定的规则、基础数据、数据映射关系,创建需要执行的数据校验任务。

c) 调度历史

对已建立的数据校验任务,进行实时的、有效的过程化监控管理,让系统分析人员能够快速分析校验任务的执行状态、执行成功、执行失败情况。

调度历史：

d) 问题数据

根据建立的规范的校验问题的处理流程,通过流程的处理流程对系统中未处理、已处理的数据质量问题进行统一管理。

3) 治理结果

提供多维度的进行数据关联,建立复杂的数据魔方地图来满足数据分析需求。

系统不仅提供基于 DB,HIVE 的 SQL 语句查询。

a) 数据配置

支持按表导入数据； 灵活的数据表拖拽、自定义条件和显示字段数据功能。能够根据不同的业务场景,自定义拼装想要的数据。

数据填报：支持模板下载,数据导入。

魔方配置：支持表拖拽,条件配置,魔方授权。

b) 数据资产

支持数据查询,数据台账,数据网盘,数据魔方,资产目录。

c) 数据查询

支持对结构化数据进行管理和查询,包括关系型数据库，HIVE。

d) 数据台账

对校验完成的数据进行统一管理和存储,可查看、导出、删除结构化数据；

支持按分类、按部门、按表进行检索。

e) 数据网盘

对校验完成的数据进行统一管理和存储,可查看、导出、删除非结构化数据;

支持按分类、按部门进行检索。

f) 数据魔方

支持按照业务跨库重新组装数据能力。

g) 资产目录

3D 动态展示目录资源与数据集之间的关系,能快速定位资源。

h) 共享服务

支持服务的创建,授权和发布。

4) 审核管理

严谨的、规范化的审核管理机制,进一步加强了元数据的有效性、合理性和易用性。

审核管理是用于审核送审的目录分类和数据集信息。包含:

审核配置:用于对审核类型的操作人员进行授权。

审核任务:对送审的数据集或目录标准进行审批。

a) 审核配置

通过审核配置,用户可将目录分类和数据集审核权限授权给审核人员,被授权人员可进行审核操作。

b) 审核任务

用户可批量审核任务或进行单条审核操作,支持目录分类与数据集的审核功能,支持审核任务的查询与查看。

5) 系统管理

系统管理模块主要提供数据源,映射关系,系统日志管理和目录分类。

a) 基础管理

提供基础数据的配置,例如:地区的配置、部门的配置、用户的配置等。

b) 数据源配置

管理员在资源库配置中设置数据库表相关信息,如:数据库表名、实例名、服务器 IP 、用户名、密码等。

支持各类数据库的连接,如:Oracle 、MySQL 能够适应目前大数据的需求。

c) 目录分类

支持目录分类的新增与管理。

HIVE,HBASE ;

d) 映射关系管理

映射关系管理:建立源数据和数据字典之间的 接关系,通过关系的建立,可查看治理后的标准数据;

支持映射关系自动匹配功能和自定义配置功能。

映射关系管理界面：

e) 系统日志

查看用户的操作日志。

系统日志界面：

（3） 功能特性

行业标准规范管理

针对数据中心的数据结构建立标准,制定校验标准、开放标准、访问标准、技术标准等。提供基于行业、主题、服务的统一标准规范制定功能,包括目录、信息类、数据元以及代码集； 为实现互联互通、信息共享、业务协同以及安全可靠提供必要前提。

全生命周期管理

支持从数据标准建立,数据质量治理,数据资产管理,数据分析整个全生命周期的数据管理能力；提供数据全生命过程的任务调度和监控能力； 提供数据资产的统计分析能力。

提供数据标准梳理工具,使得元数据更合规； 支持策略集的质量巡检方式,保障数据的完整性；建立数据治理规范体系,形成治理趋势分析。

数据存储质量

数据的存贮质量是指数据被安全的存贮在适当的介质上,采用了适当的方案和技术来抵制外来的因素,使数据免受破坏。

数据安全加固

提供全方位数据清洗,校验和加密能力,保障数据的一致性，完整性、唯一性和准确性； 提供配置化的度量规则和校验方法生成能力,提供灵活的调度执行能力； 灵活生成数据质量评估报告。

支持数据及资源级别访问安全控制,可灵活对脱敏数据进行管理。

可视化建模设计

支持可视化拖拽方式,对多种类型的数据库进行物理建模；用户可在 web 界面上进行表分类、表创建、表关系配置,支持从多元数据库中读取已有表,并配置表关系。

多维度数据管理

支持对结构化数据,半结构化数据和非结构化数据的管理和查询,包括关系型数据库表,视频,文档、图片,音频等。提供基于文本、word 的全文检索。强大的可视化文件管理能力。

支持按照业务跨库重新组装数据,查询数据,开放数据的能力。

无缝集成数据源

支持多种主流数据源的数据治理管理能力,如：Oracle 、Mysql ,Hadoop 等,实现数据源的无缝集成。

全景化信息开放与检索

支持主题的数据台账； 基于元数据的信息管理,提供 3D 数据资源目录与导航； 多渠道的数据访问机制（Hadoop、Hbase、API、Webservices ）。

7.2.6.2 数据服务集成管理系统

（1） 架构设计

SDC Publication 数据服务集成管理系统产品,旨在为用户提供符合 SOA 架构的中间件运行环境和开发管理工具。它基于工业标准（HTTP/s ,JMS,XML,SOAP ,WSDL 等） ,实现了对服务化技术的全面支持,并提供了分布式的企业服务总线 ESB 功能，确保应用系统间互联互通的可靠性和松耦合。

数据服务集成管理系统还提供了从企业应用集成的设计、开发、部署,到运行、管理、监控各个生命周期阶段的工具,方便用户充分利用 SOA 方法,解决企业应用与服务集成问题。

1 ） 体系架构图

SDC Publication 数据服务集成管理系统产品由开发工具、ESB 服务器和管理中心 3 大核心部分组成。

ESB 服务器

ESB 服务器是数据服务集成管理系统产品的运行环境,是流程、适配器、组件的运行服务器。使用者创建的流程均部署、运行在 ESB 服务器内。

ESB 总线

SOA 体系结构中 ESB （企业服务总线） 处于服务消费者和提供者的中间,提供中介功能来完成服务提供者的查找、访问、路由及服务治理等功能。ESB 总线提供寻址转换、访问、路由等常用能力。

此外,ESB 总线提供了对同步/异步等通讯方式的支持,集成了基于 JMS 标准的消息通讯方式,便于创建服务、流程间的可靠消息传递、消息的路由、和发布订阅等分布式集成应用。

流程引擎

用户使用开发工具创建提供服务中介功能的流程,ESB 服务器内置的流程引擎解释并执行流程,实现应用系统的接入和服务化,以及已有 Web 服务的中介转换。

适配器

适配器是外系统接入业务集成平台的桥梁,是多种异构系统之间互连互通及互操作的重要组件。数据服务集成管理系统提供的适配器分为入站适配器和出站适配器两类,分别用于外部应用系统调入到 ESB,以及 ESB 调出到外部应用系统。

开发工具

开发工具是用于配置中介流程、组件及适配器开发工具,它提供了完整的从设计、开发、配置到打包部署整个阶段的 GUI（Graphical User Interface ,图形用户界面） 工具 ， 帮助用户快速利用和充分发挥数据服务集成管理系统的服务中介功能。

管理中心

管理中心包括系统配置、运维、监视、服务目录 4 大功能模块,是对 ESB 服务器及部署在 ESB

服务器上面的服务、流程、共享项目等运行状况的集中监管。

管理中心采用最新互联网技术,以“服务” 为核心,在运、管、监层面支持强大的数据可视化能力。

管理中心提供 REST API,方便用户快速扩展和自行实现。

（2） 功能模块

a) ESB 服务器

标准的 ESB 总线

支持对开发 Java 代

码的在线调试功能。

内置支持开放式标准的 ESB 总线,提供服务的定义、开发、注册、认证、路由、监控、审计等功能,支持同步/异步、单向 /双向等多种服务调用及通讯方式,支持 JMS、Http/s 、等标准通讯协议和消息格式,可与消息中间件无缝集成,能够实现分布式异构系统间的松耦合,可以灵活地应对不断增加的应用集成需求,成为用户可信赖的 SOA 基础设施。

跨平台、轻量级架构

基于 Java 实现,保证了集成平台本身及创建的服务、组件和业务流程应用能够跨平台部署和运行,支持市场上常见的 Linux 、Windows 及大多数 Unix 操作系统。

采用 OSGi 轻量级架构,可以复用更多第三方应用组件,可以方便地定制和扩展适配器组件,可以进行应用组件的 “热插拔”而无需停止正在运转的 ESB 系统,方便小业务模块变更。

支持分布式应用及部署

ESB 服务器支持分布式应用及部署,用户开发的服务流程可以分布式部署到网络上的多个 ESB 服务器,实现分布式运算和应用,并支持分布式网络的可靠、安全及高效通讯和消息传输,这可以大大降低集中式部署带来的中心性能瓶颈。

支持企业级服务质量

提供对运行流程的监控诊断、错误告警等功能； 提供事务机制、跨网络的消息可靠传输和安全机制、异常补偿机制,保证事务一致性。

提供安全保障

提供了基于 WS-Security 规范的安全保护机制。提供完整的 WebService 跨网络通讯的安全机制,包括 HTTPS、WebService 访问的身份验证机制,消息加密/解密传输机制,消息的签名和验签机制,在传输层、消息层、应用层提供安全防护措施。

b) 轻量级流程引擎

可根据业务需要,使用流程引擎将多个不同服务、组件等进行编排重组,敏捷支撑面向业务的实现和重组。

支持 EIP 模型

EIP（Enterprise Integration Pattern ,企业集成模式）很好地总结了当前企业应用集成的各种模式,并提供了通用的概念和表达模型,使用户更容易完成应用集成的流程设计和模型描述， 被视

为基于消息技术解决应用集成问题的最佳实践。数据服务集成管理系统支持 EIP 模型,可以高效地解析、运行基于 EIP 模式的集成流程。

流程控制组件

提供多种流程模式控制组件,比如顺序执行、扇出、消息过滤、消息分割、内容路由、动态路由、内容丰富、异常处理、事务处理等组件,方便用户快速构建流程。

流程调度组件

提供灵活配置的流程调度功能,支持固定周期和时间表两种调度策略。

c) 丰富的适配能力

适配器是外系统接入业务集成平台的桥梁,是多种异构系统之间互连互通及互操作的重要组件。

Web 服务适配

支持 Web Service 规范族,提供调用外部系统 Web Service 的功能,提供将业务流程封装成 WebService 供外部系统调用的功能。

提供完善的安全保障,包括支持 HTTPs 协议、消息加密/解密、消息签名/验签、用户身份认证等,并提供基于 JAAS 方式的身份验证和授权扩展机制。

提供 Web Service 附件处理能力,支持将超大附件转储成临时文件的功能。

支持和 Axis 、Axis2 、CXF、.NET 等多种技术开发的 Web 服务互相调用。

支持动态路由功能。可在消息中动态指定调用外部系统 WebService 服务的地址。

JMS 适配

支持 JMS1 .1 规范,提供接收和发送消息的功能。

支持文本、二进制、键值对、流、对象等多种消息类型； 支持点对点、订阅/发布等消息模式；支持请求、请求/应答两种处理模式； 支持消息优先级、消息超时、持久/非持久等属性。

支持动态路由功能。可在消息中动态指定连接的队列名。

HTTP 适配

支持 HTTP/HTTPS 1 .1 规范 , 提供调用外部系统 HTTP 服务的功能,提供将业务流程封装成 HTTP 服务供外部系统调用的功能。

支持 REST,可以代理外部系统发布的 REST 服务。

支持动态路由功能,可在消息中动态指定调用外部系统 HTTP 服务的地址。

文件适配

支持对文件目录/子目录下变化文件的监控捕捉,提供通配符、正则表达式等多种文件匹配模式。

支持按文本、二进制、流等多种文件内容解析文件或生成文件； 支持文件内容追加、覆盖等多种输出方式。

支持文件移动、删除、重命名等多种后置处理操作。

数据库适配

提供配置 SQL 语句访问数据库的功能。

SQL 语句和参数可以动态传递； 结果数据类型可以自动转换为 DOM、JSON 等格式,便于发布数

据服务。

支持各种主流关系型数据库。

d) 丰富的处理组件

内置大量的应用集成组件,支持 EIP 表达方式,便于进行服务的封装与调用,在大多数应用场景做到零编码满足用户集成需要的服务中介功能以及应用集成功能。

消息处理组件

提供对流程中传递的消息进行处理的组件,包括对消息头、消息体、消息属性进行增加、设置、移除等处理,并支持以 Java 方式进行自定义消息处理。

数据格式转换组件

提供丰富的数据格式转换组件,支持对分隔符 （CSV） 或定长文本、XMLString 、SDO、JAXB、Byte 数组、JSON 等数据类型的转换,满足异构应用互联所需要的数据转换功能。

提供强大的图形化 XSLT 格式转换工具,对基于 Schema 的规范化 XML 进行格式转换。

支持使用多种脚本语言自定义数据格式转换功能,允许使用的语言包括：XPath、XSLT、XQuery、JavaScript 、Simple 、Method、Header、Property 、Constant 等。

e) 易用的开发工具

提供基于 Eclipse 插件模式的开发工具,可以通过鼠标拖拽或简单配置就能实现多种集成模式,用户只需要短期培训就能使用,系统上线后可自行调整,应用的灵活性大大增强。开发工具提供以下主要功能：

提供了图形化的流程编排界面,内置大量适配器、组件和控制块,可以便捷地拖曳并配置服务中介流程。

对服务逻辑和部署环境进行了抽象分离,便于在不同物理环境间迁移。

提供自定义处理组件,可以调用外部 Java 程序,便于服务逻辑与应用系统的集成； 支持 Java 代码的在线调试功能； 提供共

享项目机制,Java 程序资源可以被多个服务流程共享。

支持集成 CVS、SVN 等版本控制工具,满足团队开发需要。

f) 数据可视化监管

管理中心提供基于 B/S 架构的管理中心,采用互联网数据可视化技术,能够对服务自身以及结合业务对服务进行可视化和可操作的监视,可在监视过程中按业务和管控的需求进行操作,提

供以下主要功能：

提供对服务的历史和实时两种监视方式。

提供对单服务和多服务对比的监视模型,且多个服务可以在监视过程中增减。

提供对运行实例、服务、流程、数据源等多种对象进行监管。

提供“服务关系” 功能,能够监视到服务的访问者 IP ,并支持按业务需要录入访问者 IP 的访问者名称和访问者说明。

提供对服务的响应时间、调用情况的可视化监视,且可视化效果可操作,可在运行过程中进行实

时分析。

基于数据可视化技术实现服务的监视,提供对服务的响应时间、负载情况提供历史状态和实时状态查看功能,且所有可视化效果均可灵活操作。

提供逻辑分布、服务（业务） 分类、服务状态、接入类型 4 种默认维度的监视,并可快速扩展服务状态、访问来源等监视维度。

g）服务目录

服务目录实现了服务的统一管理,基于开发工具导出的部署包管理服务的整个生命周期,并扩展服务的业务属性,达到了将运行时资源静态化、业务化的目的。

服务注册

根据部署包（.Bar ） 注册服务,解析部署包提供服务的基本信息,并可扩展服务的业务属性的录入。

注：仅经过注册操作的服务才受到管理中心的监控。

服务查询

根据条件查询服务目录的服务列表及服务属性信息。

服务变更

修改已注册服务的属性信息,包括,变更后服务需要再此审批,如用户自身具有审批权限则无需审批。

服务撤销

撤销已注册的服务,撤消成功的服务从服务目录删除,不再受到管理中心的监控。

服务审批

服务审批包含服务注册审批、服务变更审批、服务撤销审批，严格审查服务的各项操作。

服务发布

将审批通过的服务发布到指定服务器。

服务分类管理

服务的业务属性,用户可维护服务分类树,方便服务的归类统计。

h）强开源能力

产品提供丰富 API 接口（REST） 及配套文档和示例,可基于 API 快速对产品的运行、管理、监视、权限、审计等能力进行快速扩展。

（3） 功能特性

SDCPublication 数据服务集成管理系统是一个完全符合 SOA 架构应用需要的应用集成产品,主要体现在采用 SOA 进行应用集成时所必须的服务化（Service ） 能力、架构（Architecture ）能力、以及支撑服务和架构实现的工具。

首先,SDC Publication 数据服务集成管理系统产品支持系统间松耦合的连接架构,基于工业标准,为所有需要整合的应用系统提供了统一的交流规范,并提供了大量的协议适配器,让各异构系统方便地接入总线,由总线负责协调各应用系统间的服务封装（代理） 、服务调用、消息路由,避免了

系统间接口调用关系的 耦合。

其次,SDC Publication 数据服务集成管理系统全面支持服务化技术,支持 Web 服务、代理服务,提供服务发布、注册、调用、转换、编排、监控等工具,提供了安全防护的措施,简化了服务的创建、封装、调用等繁琐的技术工作,并能够使用户灵活地编排服务,很好地监视、控制服务的运行状态和质量,以满足不断变化地业务需要和业务处理流程。

SDCPublication 数据服务集成管理系统产品功能特性如下：

帮助企业级用户快速实现多个异构应用系统的互联互通、应用集成,促进跨地域、跨部门的业务服务编排,实现业务的敏捷性。

为企业级用户可持续拓展的、松耦合的、可靠可管的 SOA 基础设施环境,支撑整个组织 IT 可持续建设与管理,实现技术的优化。

7.2.6.3 大数据展现门户

（1） 政务数据资源门户

XX 高新区开发区智慧园区政务数据资源门户 （ 内部数据门户)提供大数据平台综合展示,数据资源门户作为大数据管理部门信息发布和资源服务的总管理入口,为园区各级单位提供信息资源展示、在线信息服务、信息检索、系统集成访问等接口等。

1 ）门户基本管理

政务数据资源门户基本管理模块主要提供政务大数据中心数据成果的展示和应用访问入口的应用集成。提供单点登录、访问权限管理,后台内容管理等功能。

前端的网站页面的主要功能是面向普通用户进行访问、下载； 后台的管理系统的主要功能是面向管理员进行运营、管理。

后台管理主要分为以下几个模块：

“平台” ：对系统的全局属性进行设置。

“数据” ：对数据模块功能进行管理。

“应用” ：对应用模块功能进行管理。

“接口” ：对接口模块功能进行管理。

“移动应用” ：对移动应用模块功能进行管理。

“地理信息” ：对应地理信息应用模块的配置管理。

“互动交流” ：对互动交流模块功能进行管理。

2) 在线查询服务

系统首页提供在线查询引擎,包括一般搜索和高级搜索,一般搜索是指输入数据、应用或接口的名称进行直接搜索。高级搜索是指根据数据、应用或接口的领域、提供机构以及综合评价进行多维度的搜索。

提供面向政府部门的人口信息、法人信息、宏观经济、信用信息等信息查询服务,提供空间地理信息服务包括地图基本操作、地图测量、图层控制、空间分析以及相关数据融合等信息服

务功能。

同时在数据查询的页面提供数据、应用、接口以及移动应用的更新动态服务等。

3) 信息资源综合展示

信息资源综合展示模块通过可视化的方式展示区域内信息资源的全景,即:部门信息资源的分布情况,需求情况、使用情况等,按照不同视角进行呈现,展示内容包含:资产总体视图、组织机构视角、服务对象视角、信息资源视角、协同主题视角等。

数据地图

电子地图利用专业的地图引擎和地图底图数据,展示 XX 高新区开发区智慧园区内部数据资源,形成一张专业的智慧园区数据底图。电子底图应具备全屏、测距、测面、数据点位清除、打印/ 输出、数据查询等操作功能。

数据资源列表

展示在电子地图的数据主要分为十个大类,包括机构团体、城市建设、道路交通、经济建设、民生服务、资源环境、教育科技、卫生健康、社会发展、文化娱乐。用户可点击各类数据资源列表查看数据资源所对应的地理位置,如城市建设数据类中的全区测绘资质单位所在的地理位置,民生服务数据类中全区加油站所在的位置,机构团体数据类中的全区协会所在地理位置等。同时用户也可以通过电子地图的查询按钮,直接搜索某一个数据资源所在地理位置。

4) 用户交流模块

用户交流模块提供与政府内部用户进行互动交流的窗口,包括调查问卷、需求调查等,保证平台能够满足大部分政府内部用户的数据共享需求。

最新消息

展示政府及其各职能部门的工作动态、数据资源开放的最新消息。

调查问卷

面向用户的网站使用满意度调查或者其它业务上的调查。

需求调查

用户提交的系统新需求功能。用户在网站上未找到所需要的数据产品或应用,可以填写需求建议。比如需求标题、需求类型、功能描述、数据领域、用户类型、数据格式、用途等。

5) 用户帮助模块

为政府内部用户提供平台功能及其操作方法的介绍和帮助说明,使各级用户尽快掌握使用方法。

提供浏览器及界面分辨率要求建议,检索网站方法指南,网站乱码等其他异常问题处理办法等。

(2) 公众数据门户

XX 高新区开发区智慧园区政府公众数据门户 (外部数据门户)是建立在互联网平台上的面向社会服务的政府门户网站,搞好智慧园区政府公众数据门户网站的开发建设,是我区加大开放力度、建设服务型政府、有效实施政务公开的重要举措,智慧园区公众数据门户网站的建设对转变政府工作

职能和工作方式、提高服务水平,建立与经济社会发展和对外开放要求相适应的工作体系,具有重要的作用。

本次新增智慧园区数据开放专题模块将在原有网站系统上增加数据专题应用展示窗口,公开各类数据的下载与服务,为企业和个人开展政务信息资源的社会化开发利用提供数据支撑接口,推动信息资源增值服务业的发展以及相关数据分析与研究工作的开展。

公众数据门户的主要功能有：资源目录、数据开放接口、APP 应用、互动交流等。

1 ） 资源目录

资源目录模块提供社会公众通过资源目录查找到需要的数据,找到相应数据的获取方式,社会公众可以通过数据下载,数据接口等多种方式进行获取,公众获取数据时必须提供用户注册认证机制。用户可以通过数据资源主题,数据来源部门等多种方式进行查找。

用户可以在系统中进行数据搜索,系统首页提供搜索引擎，包括一般搜索和高级搜索,一般搜索是指输入数据、应用或接口的名称进行直接搜索。高级搜索是指根据数据、应用或接口的领

域、提供机构以及综合评价进行多维度的搜索。

同时在数据搜索的页面提供数据、应用、接口以及移动应用的更新动态。

数据搜索的页面提供数据更新动态、数据下载动态以及数据评价动态等实时动态数据。

数据下载使用由平台管理单位提供数据使用条款,包括用户义务、接受条款、隐私保护、免责声明等。

资源目录提供数据地图查询服务,查询全区各主要事业单位、政务服务机构、主要机关团体以及民生服务机构的地理位置等。

数据地图

电子地图利用专业的地图引擎和地图底图数据,展示智慧园区政府数据资源,形成一张专业的智慧园区数据底图。电子底图应具备全屏、测距、测面、数据点位清除、打印/输出、数据查询等操作功能。

数据资源列表

展示在电子地图的数据主要分为十个大类,包括机构团体、城市建设、道路交通、经济建设、民生服务、资源环境、教育科技、卫生健康、社会发展、文化娱乐。用户可点击各类数据资源列表查看数据资源所对应的地理位置,如城市建设数据类中的全区测绘资质单位所在的地理位置,民生服务数据类中全区加油站所在的位置,机构团体数据类中的全区协会所在地理位置等。同时用户也可以通过电子地图的查询按钮,直接搜索某一个数据资源所在地理位置。

2) 数据开放接口

数据开放接口提供整合全区现有业务数据的对接地址及接口文档,便于用户单位对接数据,同时平台管理员需要保证各接口的有效性,提供数据接口介绍,并对各个接口进行分类统计。

3) APP 应用

公众数据门户移动应用系统（APP）,提供系统登录网址、系统主管单位、系统评分等,同时平台管理员需要保证各整合系统的正常使用,并对个应用系统进行分类。移动应用系统提供安装包下载地

址。

4）互动交流

互动交流模块提供网站管理人员与网站用户进行互动交流的窗口,包括调查问卷、需求调查等,保证平台能够满足大部分用户的数据共享需求。

最新消息

展示政府及其各职能部门的工作动态、数据资源开放的最新消息。

调查问卷

面向用户的网站使用满意度调查或者其它业务上的调查。

需求调查

用户提交的系统新需求功能。用户在网站上未找到所需要的数据产品或应用,可以填写需求建议。比如需求标题、需求类型、功能描述、数据领域、用户类型、数据格式、用途等。

7.3 实施方案

7.3.1 项目组织实施

（1） 实施原则

在项目的整个实施过程中,公司设立的项目领导小组将按照以下原则开展实施工作：

1）以客户为中心,在本项目招标文件约定的范围内,全面了解和摸清用户需求,实现用户需求；

2）规范实行项目管理,以保障项目的顺利进行；

3）组建优秀的项目组织机构。

（2） 施工组织

项目领导小组负责监督、协调项目经理、质量保证小组。同时,项目领导小组也负责协调项目经理反馈的由项目经理无法协调的事项。项目领导小组成员由我公司和客户相关部门负责人组成。我公司项目领导小组成员负责对整个项目的工程预算、工程进度、工程质量等进行审核批准和监督,负责合理调配公司内人力及物力资源,提供必要的人员配合、协调项目经理和质量保证小组的工作、并监督整个工程进度。以确保本工程高质量、高效率、顺利的进行实施。

（3） 实施工期

项目要求自合同签订之日起 180 天内完成项目的设计实现，另外 60 内完成项目的安装实施。

（4） 进度计划

（5） 工期管理

通过建立项目进度计划管理和控制的模式、工作程序和工作方法,促进项目工期管理工作科学化、规范化,提高进度计划管理和控制的工作效率、质量和水平。用于本次项目从需求调研到验收交付、

后期的运维服务整个过程的工程计划管理。

（6） 主要内容

主要内容包括四个部分：

1 ）计划：针对本项目指定详细的实施方案和计划；

2）实施：各阶段设计方案、测试方案、质量管理方案,实施过程记录、质量管理记录、资源调配；

3）检查：实际进度和计划对比,分析偏差原因,及时调整；实际质量与设计质量对比,分析偏差原因,及时改进；

4）总结：各阶段总结,使之标准化、制度化,同时按计划进入下一个管理循环。

（7） 职责分工

工期管理与控制实行分级管理。公司负责制订和完善管理制度,并对项目进行管理、监督； 项目经理负责项目实施管理,汇总上报管理情况,协助投诉处理。

（8） 公司职责

1 ）制订和完善工期管理办法,建立项目工期管理体系；

2）审核施工总进度计划、成本计划、预算计划和奖惩制度；

3）负责项目管理人员的配置与优化、管理与调配；

4）建立项目工期管理的报表制度,监督检查项目进度动态管理,审核月 度进度计划完成总结,并提出整改意见；

5）对项目进度管理和控制进行定期考核,视情况进行奖罚；

6）受理进度或工期投诉,督促对存在问题的整改；

7）接受工期管理情况报告,并对本办法执行情况进行监督与处罚；

8）人力资源关键绩效指标分析与评价,并根据评价结果提出对策。

（9） 项目经理职责

1）依据合同、项目策划、项目计划的约定,组织项目总工程师（技术负责人） 和相关管理人员,编制项目详细设计、施工进度计划和施工进度计划；

2）确定项目节点控制办法,明确工程节点,并确定奖罚；

3）审核项目实施关键线路,制定节点控制目标和项目施工进度计划编制说明书,签字并上报；

4）依据项目 计划,组织编制项目 季/月/周进度控制计划；

5）组织或授权组织项目例会,掌握项目进度,并上报；

6）组织项目管理人员、质量控制人员、测试人员定期检查进度计划完成和质量情况；

7）组织编写、审核周、月 度进度控制报告,签字并上报。

（10） 质量管理人员（QA） 职责

1）在项目经理和技术负责人的领导下,依据 CMMI（Capability Maturity Model Integration ,软件能力成熟度集成模型） 和公司研发质量管理制度,制定项目 质量管理计划和检查列表；

2）定期、不定期对项目实施情况进行检查,及时发现问题，提出整改意见；

3）编制项目周、月 、季度质量控制报告。

（11） 任务分解

1 ）进度控制目标分解

项目经理组织项目进度控制管理人员确定项目进度控制目标和进度计划,并进行进度节点目标分解；

项目经理分解任务目标到团队个人或小组。

2）实施进度计划

依据分解任务目标,制定实施工作计划和质量计划；

制定风险控制计划。

（12） 过程控制

周期计划检查：对关键线路进行周计划检查,包括进度、质量和风险,及时发现问题,提出整改建议； 对于严重风险,及时制定风险控制措施；

关键点控制：对关键点完成情况进行检查,对发现的问题提出整改建议或风险控制措施；

质量控制：组织 QA 对项目实施质量进行检查；

控制报告：编写过程控制报告。

7.3.2 突发事件处置

（1） 技术风险

技术、产品更新不及时风险

公司坚持进行技术创新和积累,加强新技术研发力度,加大科研投入,并与多家高等院校、科研院所进行合作,不断提升公司的技术研发能力。同时,加强技术积累和沉淀,不断完善技术产品,确保产品和技术稳定、高效。

核心技术人员流失的风险

公司核心技术人员的技术水平和研发能力是公司能长期保持技术优势的保证。业内的人才竞争日益激烈,能否维持技术人员队伍的稳定,并不断吸引优秀技术人员加盟,关系到本公司能否 续保持在行业内的技术领先优势和未来的行竞争力。公司在提高技术人员薪酬和奖励的基础上为其提供良好的科研条件和发展空间,最大限度降低人才流失风险。针对本项目,关键岗位人员采用双备份策略,确保项目顺利进行。

知识库

对核心技术,业务经验等关键知识,采用知识库形式进行积累和沉淀,即使人员变更,后续人员也能通过知识库,快速掌握相应知识和技能,从技术上保证项目的顺利延续。

（2） 人员风险

保证开发组中人员合理配置,且项目核心部分的工作公司骨干人员来担任,以减少人员不稳定性的影响。

建立良好的文档管理机制,包扩项目组进度文档、个人进度文档、版本控制文档、整体技术文档、个人技术文档、源代码管理等。一旦出现人员的变动,替补的组员能够根据完整的文档尽早接手工作。

加强项目组内技术交流,比如定期开技术交流会,或根据组内分工建立项目组内部的开发小组,是开发小组内的成员能够相互熟悉对方的工作和进度,能够在必要的时候替对方工作。

对于项目经理,从一开始就指派一个副经理在项目中协同项目经理管理项目开发工作,如果项目经理退出开发组,副经理可以很快接手。

为项目开发提供尽可能好的开发环境,包括工作环境、待遇、工作进度安排等等,同时优秀的项目经理在项目组内营造一种良好的人际关系和工作氛围,良好的开发环境利于稳定项目组人员以及提高生产效率。

（3） 需求风险

在设计初就已经考虑可能存在的需求变更风险,系统采用模块化体系架构,将需求变更带来的影响降到最低。同时在计划制定时,预留了一定的需求变更处理时间。系统采用严格的版本控制策略,对变更的需求做详细分析和控制,将变更的实现放到最合适的版本中,这样便于版本的稳定和新版本研发。

（4） 计划风险

项目制定工作计划时,可能因各种因素,存在进度偏差,导致整个项目实施计划存在风险。对此,在项目实施过程中,设置不同的关键节点,定期或不定期对关键节点进行检查,通过完成情况和质量,分析可能存在的计划风险,及时采取应对措施,确保整个项目计划顺利进行。项目例会、QA 检查计划也是风险控制策略。

（5） 质量风险

项目研发过程中,由于各种因素,可能带来质量风险,针对该类风险,本项目采取的策略主要包括:

QA 检查：严格按照 CMMI 质量要求进行过程质量检查和控制， 及时发现问题,提出整改建议;

技术测试:通过对研发成果进行全面的单元测试、集成测试和系统测试,最大限度降低质量风险。

（6） 其他风险

我公司通过丰富的技术积累,充足的技术人力配置,完善的管理制度,能够快速应对项目实施过程中可能出现的各种风险， 最大限度保证项目顺利实施。

7.3.3 项目验收

（1） 整个系统开发完成,安装调试完成后,所有功能、性

能指标达到双方确认的技术规范要求时,进入系统的整体试运行

期;

（2） 系统试运行期间,所有功能、性能指标达到双方确认的技术规范要求时,我公司向业主提出终验申请,填写项目终验申请表以及验收方案,并至少提前 1 0 日提交给采购人,双方对验收方案进行确认；

（3） 由双方共同进行系统的最终验收。终验包括对所有交付品的检查、功能验收及性能验收；

（4） 终验合格后,经双方确认,形成终验报告,由双方项目负责人签字生效。

7.3.4 项目交付

交付文档包括技术文档、测试验收文档、培训文档、服务文档、会议记录文档。交付内容详见“项目验收标准和方法”.

7.3.5 项目管理与质量保障

（1） 项目管理组织

针对本项目,我公司在施工前安排硬件工程人员配合采购方对已有服务器、网络线路、网络硬件实行工程验收和工程监理，保障后续软件稳定运行。

针对本项目,成立相应的工程指挥小组,并指定一名专职的项目经理,负责工程协调和调度工作（包括中标后,代表采购方进行信息基础硬件的施工监理和验收） 。成立包括一名专职项目经理在内的技术支持小组,负责对参与项目实施的各方技术人员进行产品、技术培训,提供项目整体实施和试点工作的技术方案，对工程实施过程中出现的疑难问题提供技术支持。

成立的组织机构包括：需求分析组、系统设计组、系统研发组、系统设计组、系统维护组、质量管理组、文档编写组、技术支持组、技术培训组,每个小组由经验丰富的人员组成,在统一软件研发和工程管理质量体系下,各小组分工合作,对项目进行规范化管理,提供项目管理计划、项目进度计划、项目验收计划等方案,确保工程实施质量,并全力配合项目集成商的总体集成工作。

人员稳定性保证

项目组成员为公司自有人员,在未经过项目建设单位同意的情况下不得私自更换开发人员。

人员经验保证

公司针对该项目建立实施该项目的组织架构,项目经理及其团队成员具有类似项目经验。

人员现场保证

为保证本项目的顺利实施,所有与本项目相关的实施工作，公司都在现场实施。

（2） 实施过程管理

经验丰富的实施团队,采用经过大型复杂项目验证的实施方法对项目实施过程进行控制与管理。在项目实施过程中,需要重点关注需求、设计、实施阶段的里程碑节点,把好进度质量关，控制好风险,解决好偏离等,使项目实施过程基本按照设定的轨迹进行,从而保证整个项目的实施。

（3） 过程管理策略

建立项目例会制度

由项目经理每周召集举行项目组内部例会,对项目实施工作完成情况进行总结并确定下周计划,同时在会上对提出的争议和问题进行讨论。由项目经理根据项目情况召集举行项目月 度例会,主要讨论总体的项目进展、问题和变更的状态、后续的工作进程和任务分配等并形成会议纪要。在实施过程中发生的临时性会议,视情况随时召集。

注重前期服务和事前策略

发挥公司的综合优势,提供规划、科研、咨询等专业支持。

针对具体建设内容,根据业主的基本设想,主动帮助解决项目建设中相关问题,从规划、设计、施工、部署、测试等进行全面研究,为未来项目建设提供有效的参考。

抓好全面控制和精细管理

针对不同的项目要求,从管控机制、过程管理和项目保障等方面,提高项目管理的能力。构建项目管理机构,实行决策支持、规划管理、技术实现三级管理体系,落实人员和相关的职责,发挥综合实力。编制实施方案,根据项目实际情况,分析项目概况及其特点、难点,总结各个功能、流程、主要技术路线、实现方法等,使整个项目的实施按计划、按规范进行,确保项目进度总体受控。统一有关的制度、标准和流程,包括文档编写基础类模板、需求规格说明书类模板、设计文档模板类、测试方案模板类、信息平台软件验收标准、支撑类软件定制实施规范、软件技术实现规范、公共配置管理规范、统一用户管理规范、周报制度等，确保各系统承建单位的工作有序进行。

重视原则建立实施规范

本项目建设服务是一个复杂而庞大的系统工程,尤其需要所有参与人员不断开拓新途径和新的突破点,把握系统建设的基点,抓住系统实施的重点,重视实施建设中应遵循的原则,建立实施中要遵从的实施规范,做到项目实施精细化管理。

（4） 项目范围控制

项目范围是一个大致的范围,须根据用户需求进行详细的需求调研,从平台的组成、技术需求、业务应用需求、安全需求和管理需求等方面进行详细的需求调研、整理和确定,形成详细的需求规格说明书。项目实施过程中,严格按需求规格说明书进行项目范围控制,并对需求变更拟定相应的应对措施和策略。

（5） 项目变更控制

对于软件开发项目而言,变更一般是不可避免的。为了将项目变更的影响降低到最小,采用 CMMI 体系的变更控制方法。变更控制就是要找出影响项目变更的因素、判断项目变更范围是否有必要、判断项目变更的结果是否已经发生及效果如何等。进行变更控制的主要依据有：项目计划、变更请求和提供了项目执行状况信息的绩效报告。

（6） 项目质量控制

质量控制的目的是保证项目成果的质量满足项目质量计划中说明的项目成果的质量要求。项目质量计划的说明可能会引用其他文件来说明项目成果的质量要求,如招标书、投标书、合同、需求规格说明书、国家标准、行业标准、企业内部制定的各种规范等等。为保证项目的实施质量,将从质量

保证、配置管理、测试管理等方面建立相应的管理体系,从多个维度来保证项目能够按照质量要求和时间计划成功完成。

1 ）质量保证体系

本项目中采用统一标准,明确定义保证项目质量的责任和方法,结合项目的实际情况,质量保证和责任划分。每一大类或一个阶段的工作内容结束后,做工作总结和定期的状态报告会,以保证客户和项目负责人能及时跟踪工作的进展。另外针对软件开发质量保证,其主要任务是软件过程的审计,主要内容包括：

1） 评估各阶段的评审过程；

2） 评估项目计划和监督过程；

3） 评估并监督软件开发工作的执行；

4） 评估需求分析过程；

5） 评估设计过程；

6） 评估编码和单元测试过程；

7） 评估部署集成联调测试过程；

8） 评估项目最终交付过程。

2) 配置管理体系

整个项目的各小组按照统一的配置管理要求,各自做好配置管理工作,并建立专门的配置管理服务器,对项目过程中的所有成果实行配置管理。项目过程中输出,按统一的配置管理要求进行配置管理。

配置管理包括：交付产品的确认、软件模块的版本控制及其交付与发表、各种状态（开发、测试、集成、验收、维护） 中的

变动记录等。在项目实施过程中,配置状态提供充分的可视性，确保相关人员在任何时刻都能采用正确和准确的信息。

3) 测试管理体系

依照 CMMI 和质量管理体系,建立完善的测试管理体系,主要过程包括：测试方案编制和评审,测试用例编制和评审,测试输出和问题记录,回归结果和测试报告,每个过程都具备详细的记录。

（7） 项目进度控制

项目进行过程中,不断检查、监控项目的进展情况,以保证每项分解的任务都能按计划完成。持续收集项目进展数据,掌握项目计划的实施情况,将实际情况与进度计划进行对比,分析其差距和造成这些差距的原因,必要时采取有效地纠正或预防措施,使项目按照项目进度计划中预定的工期目标进行,防止延误工期。项目进度控制不仅要注意主要任务或关键路径上的任务的工期,也要注意一些本来次要的任务的进展,以防止次要任务拖延,影响主要任务和关键路径上的任务。主要措施包括：

1 ）项目例会

每周召集举行有业主单位参加的项目例会,汇报项目进度和下周计划,同时在会上对提出的争议和问题进行讨论。在实施过程中发生的临时性会议。

2) 项目状态报告

在项目实施过程中,及时提交项目状态报告,汇报项目的进度以及完成、未完成工作、存在问题、下一步的工作计划等内容。

3) 项目里程碑/阶段评估验收

在项目的需求分析、系统设计、项目验收等里程碑点,组织完成需求分析评审、设计方案评审、集成支撑软件设计方案评审、集成相关技术规范评审、项目验收等内容。

（8） 项目成本控制

成本控制的基础是在项目计划中对项目制定出合理的成本预算,并尽可能地保证各项工作在项目计划中预定的预算内进行。软件开发项目的成本最主要的是人力资源的成本,而人力资源的成本体现为各个项目成员薪资水平乘以他所花费工作日的总合,因此人力资源的成本其重点在于合理地安排使用合适的人力资源。软件开发项目 的成本还包括购买必需的软硬件设备的成本;

需求调研所花费的交通、协作、通信成本； 购买必要的办公用品、参考资料的费用； 给用户培训所需要花费的培训资料编写费、资料印刷费、产地费、设备费； 如果需要第三方的鉴定或检测,还需要一定的鉴定检测费用； 进行质量、进度控制的管理成本。

（9） 沟通管理

为保证项目参与各方准确把握项目进度情况,指定相应的沟通策略。

1 ）汇报管理

定期或不定期的向业主汇报项目进展情况,需要业主协调解决的问题等,主要方式是通过项目例会,也可以通过不定期会议。

2) 沟通管理

常用的沟通方式主要有：现场办公、监理例会、专题会议、电子邮件、QQ 网上通讯、手机通讯等。

沟通内容

与计划相比,项目工作量完成情况;

已完成的工作质量情况;

项目执行过程中出现的问题,以及解决方案和建议。

报告形式

报告使用 PPT、Excel 表格、Word 文档等方式。

相关文档

项目沟通管理产生的相关文档包括但不限于：

《会议纪要》 ,包括：会议时间、地点、与会单位及人员、会议议题、会议结论、会议遗留问题等;

《项目周报》 ,包括：项目名称、周起止时间、一周工作内容、遇到的风险与问题、下周工作计划等。

第八章 智工业园区治安防控情报信息上报

8.1 社会化警务助理信息上报

智工业园区社会综合治理云平台一个核心业务在于智工业园区警务助理、信息员、巡防安保人员的社会治安防控情报信息实时上报。这些信息包括但不限于社情民意搜集、矛盾纠纷排查调解、案件线索、非法集资/非法集会/吸毒涉黄信息、治安隐患点、违法犯罪行为、警情等。上报方式是在管理服务对象的移动终端安装 APP,服务管理对象在该 APP 的管理下采集提报信息,APP 是信息的源头,APP 与智工业园区社会综合治理云平台平台之间的互动是通过消息推送服务器，APP 首先将信息发送至消息服务器,消息服务器将推送至智工业园区民警的互联网 APP 端或值班电脑 PC 端。APP 上报信息以点对点方式发送给上级智工业园区民警,确保信息安全不被泄露,同时会关联上报人员坐标信息,通过消息方式传送至智工业园区社会综合治理云平台在地图上显示。同时通过数据库服务方式将上报详细信息推送至平台数据库中,在地图上的气泡框中可点击查看信息详请。

智工业园区民警利用互联网终端对所管理服务对象提报的信息进行查看、反馈、提报,对管理服务对象有价值信息自动纳入公安网相应后台进行流程处理,管理服务对象登陆 APP 能够查看自己的报送的信息并查看智工业园区民警反馈。

8.2 信息图上展现

智工业园区民警通过互联网 PC 端,实现所辖区域信息的图上集中管理,过去一段时间的信息在图上撒点展现,并同时以列表方式排列显示。信息提供分色管理、根据信息的类别、是否已经接收等不同状态在地图和列表中进行不同颜色的展示。

8.3 服务管理对象定位信息管理

系统内部建立定位信号与设备信息、服务管理对象人员信息、组织机构信息之间的动态关联,并实时存储定位信号形成轨迹库。

服务管理对象与装备关联

通过组织机构实现对服务管理对象终端的管理,实现对终端设备与服务管理对象进行关联管理。

实时轨迹存储

提供智能终端设备位置信息的集中存储服务,对每个终端进行分布式坐标信息的存储,并最终形成历史定位资源库,支撑业务应用中的轨迹查询浏览、轨迹碰撞分析等业务实战应用。

8.4 服务管理对象定位上图

将系统后台实时接收到的海量定位信号,通过消息总线推送到互联网客户端 （智工业园区民警APP 端和 PC 端） ,并实时的撒点到地图上； 同时可基于组织机构及范围进行服务管理对象查询和人员基础信息显示。

根据业务对服务管理对象状态进行归类,智工业园区民警可以在电子地图上实时监控辖区内人员位置及状态信息 （用不同颜色代表不同人员状态信息） 。直接点击任意人员目标图标,可显示目标信息。显示所有移动目标的最新运行状态 （ 经纬度、速度、时间、状态、监控属性等 ） 和相关信息 （ 名字、组织单位、工作岗位等 ） 。

8.5 视频监控集成接入网关（可选）

本方案通过部署专用视频监控集成接入网关,把智工业园区内不同类型的视频监控系统通过GB/T-281 81 协议、ONVIF 协议、RTSP 协议、SDK 等多种方式接入到智工业园区社会综合治理云平台,具备视频和音频码流的分离、转发、SIP 代理封装功能 ， 可通过互联网 APP 端和 PC 端实现对现场监控图像的调度,同时可把调度回来的图像转发/分发到其他视频接收单元显示。

8.6 图上周边资源查询

图上周边资源查询,在地图上通过目标点周边筛选资源,同时支持圆、矩形、多边形、任意区域绘制等条件,筛选框将展示该区域附近所有的智工业园区、医院、学校、重点单位、特种行业等,点击列表中的资源信息直接居中定位到地图上,同时显示资源的详细信息。

8.7 通知公告

智工业园区社会综合治理云平台具有通知通告下发功能,实现对服务管理对象按组织机构或巡防区域或单点下发通知公告，并会以声音、消息等方式提示用户查看指令。通知通告发布可以发送文字、图片、多媒体信息等。

8.8 逐级精细管理模式

建立网格管理层级,形成市、区县、街道、XXX 区社区、网格五级管理模式,深化管理层次、强化管理层级。设置网格管理层级后,一个 XXX 区社区按照地域特点、管理类型等划分为多个网格,缩小的管理范围,易于情况的掌握与处理。

8.9 事件上报

由群众（通过手机终端） 、楼长、网格长等将发生的事件 （包括市容环境、违章宣传广告、非法施工建设、突发事件、街面秩序、以及民事纠纷等等） 进行上报,平台将自动记录事件的上报时间、上报人、事件内容记录、涉案甲方和乙方、性质等等信息，进行数据入库。

8.10 平台事件自动分流

台根据已上报事件的内容和性质,验证分流开关（关闭和开启） 后,进行自动分流处理将所上报的事件分配到各个适合部门进行处理。

8.11 绩效自动考核

对各部门、乡镇、行政综治进行自动考核,并按所设置的时间进行列表和统计展示；

8.12 事件项目可定制

此平台根据事件所发生的性质,按所设置的时间进行查询和分类使其一目了然,便于对整个 XXX 区社区的事件管理和评估。

8.13 接口开放

此平台将提供其他平台数据访问的接口,将采用 HTTP 协议，HTTP 具有支持客户/服务器模式,支持基本认证以及安全认证，快捷方便、灵活等特点,接口将以 JSON 数据类型发送给其他平台,达到信息全面、快速、安全、简便等访问特点；

8.14 GIS 可视化操作

平台具有放大、缩小、移动、视野控制、中心移动、图层控制等功能,使操作更加灵活、更加方便简洁。

家庭及人口的定位查询：

平台可以根据你要查询的户或人的信息在地图上进行定位和高亮显示且将查询结果以列表显示,也可以根据地图进行反向查询,及点击地图的某一区域可以查询出这一区域的所有信息且进行列表显示。

事件发生地点定位查询：

根据库存的事件信息,将要查询的事件进行定位点状显示，同时将整个事件信息进行展示,同样

可以进行反向查询。

专题图显示：

将所查询的人员、户或者事件信息进行不同颜色的专题图显示,使查询结果直观、清楚明了；

8.15 符合规范

平台符合中华人民共和国城镇建设行业标准和《数字 XXX 区社区管理与服务》条款,融入了 XXX 区社区管理、公共服务、商业服务、单元网格、责任部门等多种网格化建设管理,符合《数字 XXX 区社区管理与服务》 的网格划分原则及编码规范。地理编码符合。

第九章 服务管理对象一键报警（可选）

9.1 服务管理对象互联网 APP 端一键报警

服务管理对象可对现场巡逻、执勤发现的警情,进行一键式快速上报。自动上报智能终端所在地点坐标、上报服务器自动生成警单。

9.2 警情进入三台合一接处警

实现与市局三台合一系统警情数据的对接,实现警情数据实时同步上报； 支持中间库对接、Socket 对接、MQ 对接、WebService 对接方式,并支持正向及正反向数据实时更新。

通过接处警系统接受到报警人员坐标信息,通过消息方式进行传送至智工业园区社会综合治理云平台在地图上同步显示。同时通过数据库服务方式将警单详细信息推送至平台数据库中,在地图上的气泡框中查看警情详细信息。

9.3 警情状态更改

警情状态分色管理、服务管理对象互联网 APP 警情状态与三台合一系统实时同步,根据警情所处的接警、出警、到达现场、处置结束等不同状态在地图和列表中进行不同颜色的展示。

9.4 辖区手动扁平派警

警情所属辖区分局或派出所指挥中心在平台 PC 端监测到新接报的警情后,可以通过警情的派警按钮,系统自动将所属辖区的处警执勤警力以列表形式在警情右侧动态展开,派警人员只需选择所要派遣的警力编号,即可完成手工派警。

系统会自动将所属辖区的处警执勤警力以列表形式在警情右侧动态展开,派警人员只需选择所要派遣的警力编号,即可完成手工派警。

9.5 图上就近扁平调警

可以通过警情的图上调警按钮,实现在警情发案地点附近快速检索周边警力,通过图上圈选警力,系统便自动将派遣指令推送到一线

同时,系统在图上以动态连线的形式将所有被派遣警力与目的地直接连接,以便用户可以清晰了解被派警的警力和目的地情况。

9.6 警情警力实时态势

针对警情流转的不同环节,系统能够按照不同颜色展示当前警情的处置状态,包括:接受新警单、确认前往出警、到达现场以及处置完毕等。实现对警单不同处置状态的分色管理。并对各单位的警情处置的时间进行统计考核。

警情态势监控

系统中对所有接收到的警情以“红” 、“黄” 、“蓝” 、“绿” 四种颜色分别代表“未处理” 、已派警且警员已“签收” 、“到达现场” 、处置“完成” 四种实时的警情细分状态。

警力态势监控

警力分色管理与警情分色管理相对应,以“黄” 、“蓝” 、“绿”三种颜色分别代表“签收” 、“到达现场” 、“空闲” 三种实时的警力细分状态。

9.7 人口管理

人口管理是城市政府对城市常住人口户籍和人口变动的行政管理工作,以及对城市人口的数量和质量、人口与计划生育以及流动人口等管理。城市人口管理对我国市政建设有着重大的现实意义:首先,城市人口管理是城市政府的重要职能之一。其次，加强城市人口管理是城市发展的客观要求。再次,加强城市人口管理是充分发挥城市功能的有力保障。最后,加强城市人口管理是维护城市正常生产生活秩序的必要条件。人口管理可以实现如下三个方面：其一、贯彻计划生育的基本国策。其二、控制城市人口的机械变动。其三、实现对城市流动人口全面统一的管理。

9.8 特定人口管理

对于孤寡老人、残疾人、老年人、未成年人、妇女、最低保障对象、下岗失业人员、革命伤残军人、复员军人、因公牺牲军人家属,病故军人家属、现役军人家属、军队离退休干部精神病人、吸毒人员、违法青少年、流浪儿童等特殊人群,要分门别类、以类施策,区别对待、因材施教,最大限度地把影响社会的消极因素转化为促进社会稳定的积极因素。以在城市建立流动人口公共服务与保障体系。

9.9 单位法人管理

通过对单位法人进行管理,我们可以定期或不定期的对商户发送信息来通知法人。

9.10 XXX 区社区单位管理

在 XXX 区社区之内,凡对个人有其重要性的种种经验和活动，其中大多数都能够亲身去体验和

活动,其中大多数都能够亲身去体验和处理。XXX 区社区生活是一种共有、共治、共享的生活。

个人的生活方式及人格发展,受 XXX 区社区组织的影响,至钜且深。XXX 区社区内各个人间发展出两种意识：一是本土意识—个人在此土生土长,根深蒂固； 一是证同意识 ， 都属于此一 XXX 区社区,各个人的特色,即代表 XXX 区社区的特色。各个人在 XXX 区社区内休戚相关,祸福与共,有‘一家人’ 的感觉,对 XXX 区社区的接受,极为率真自然,如同接受自己的姓名和家中地位一样。所以建立 XXX 区社区组织有助于更好的维护 XXX 区社区团结,互助。

9.11 商户管理

商户管理是指对商场或专业市场内经营的独立经营商户的管理。通过对商户进行管理,我们可以定期或不定期的对商户发送信息来通知商户。

9.12 民情上报

民情上报是农村基层干部转变工作作风,密切同群众联系， 帮助农民排忧解难,解决实际问题的一项有效措施,是干部联系群众的一种好形式。首先,民情上报弥补了工作日志的不足,它不是工作日志的简单罗列,不是事件的堆砌,也不同于个人日记；

民情来源于日常工作而又超越于日常工作之上,它是在真实地反映社情民意的基础上,以下派干部在工作中的感受和经验为主，结合实际去分析和研究下派工作中的问题,是下派工作中的现象和问题的升华,具有较强的思想性和可读性。通民情上报可以随时随地记录民众间发生的事情。

9.13 警情上报

对社会发生治安、犯罪事件后,必须由警察出警察来维护社会稳定的突发性事件,或者说是危害公共安全的事件。各地的“警情” 和警察的出警数是衡量一个地方治安以及社会稳定的只要因素之一。“警情” 并不是警察的主观行为,而是当社会出现治安事件后使警察出警的一种客观的存在。通过警情上报 ， 可以对该事件进行记录 ， 留到日后对该地区的治安进行统计和分析。

9.14 自动考核

为了提高 XXX 区社区工作人员的积极性和工作态度,采取考核机制,通过对 XXX 区社区工作人员的工作内容,处理数量,处理结果及处理反馈运用特定的标准和指标,对员工的工作行为及取得的工作业绩进行评估,并运用评估的结果对 XXX 区社区工作人员将来的工作行为和工作业绩产生正面引导的过程和方法。

通过考核,把 XXX 区社区工作人员聘用、职务升降、培训发展、劳动薪酬相结合,使得企业激励机制得到充分运用,有利于 企业的健康发展； 同时对 XXX 区社区工作人员本人,也便于建立不断自

我激励的心理模式。

9.15 自动统计

统计可以对人口信息,特殊人群,公告安全,XXX 区社区组织的相关需要统计的数据进行图表统计,以对一段时期内人口信息的变化趋势或 XXX 区社区内特殊人群等的变化进行统计,来对这段时期内发生的变化进行分析,以做出最优决策。例如：对小区内偷盗、吸毒、斗殴事件,进行统计,来分析小区的公告治安问题,或是这些事件多发地带进行更好的处理及管理。

9.16 自动通知

在业务处理过程中,对我们需要下发的信息进行发送 （包括邮件和短信息） ,更好的对每个处理过程进行下发工作人员处理信息进行处理或是对普通民众下发通知信息来进行告知。

9.17 自动催促

在业务处理过程中,对一下还未处理或还没有处理完成的事件进行催促（以短信或邮件的方式）

9.18 流程定制

通过流程定制,可以对平台的事件处理流程进行自动或是人工操作,这是个由易到难的操作,对于平台的自动操作,是有平台自动进行分配事件进行操作。而人工操作是由人进行事件的分配,并且可以对事件更好的处理。

9.19 事件定位

进行事件上报时,对事件进行地理定位,以便更好的确定发生地区,来通知就近的人或使用就近的物进行事件处理。更可以通过统计对该某一区域发生的事件进行统计。

9.20 人口定位

通过对移动设备的监听或是设备实时的发送自己的位置,来进行 XXX 区社区人员的定位,以防人员丢失或突发情况,以做到快速解决问题。

9.21 事件流程跟踪

对于事件上报之后事件处理的一切流程都做相关记录,用来实时查看事件处理的情况。来做出相

应的处理和催促。

9.22 分级管理

通过分级管理,实现上级对下级的管理及上级和下级的分工协作。这里体现的是乡镇对 XXX 区社区的管理,XXX 区社区对网格的管理,网格对小区的管理及小区对楼的管理,来实现层级管理。这样可以更好的事物细分,责任归属到位。

9.16 自动通知

在业

9.23 老人和儿童管理

面对我们身边的弱势群体,我们采取对他们的特殊监管,通过移动设备,对老人及儿童进行实时的监管,对老人的需求实时的处理。对小孩的坐标进行实时的定位。

9.24 公共安全管理

公共安全是指多数人的生命、健康和公私财产的安全。破坏公共安全的行为是指故意或过失危害不特定多数人生命健康和重大公私财产安全的行为。我们通过上报事件信息进行分析处理,来解决公共安全问题。

9.25 邻里矛盾解决

在对发生事件分配后,由专人负责解决邻里矛盾,邻里问题是我们生活在一个社会大家庭,楼区小家庭必不可少的交际问题,对于邻里之间的矛盾应该及时的解决,以便促进邻里和谐。

9.26 舆情监控

整合互联网信息采集技术及信息智能处理技术通过对互联网海量信息自动抓取、自动分类聚类、主题检测、专题聚焦,实现用户的网络舆情监测和新闻专题追踪等信息需求,形成简报、报告、图表等分析结果,为客户全面掌握群众思想动态,做出正确舆论引导,提供分析依据。

9.27 XXX 区社区环境监控

环境监控是环境保护及管理工作的重要基础,随着经济的快速发展,越来越多的人开始关心所处

环境质量的好坏,要求环境保护及管理工作的效率提高、质量提高、加大透明度。通过信息化技术的应用,改变传统环境监测手段,运用新的通讯网络技术对污染源及环境质量实施长期、连续、有效监测,科学准确、全面高效地监测、管理所辖区域的环境状况,使环保部门的环境管理工作达到监测科学、管理高效、执法公正的新境界。

9.28 黄赌毒及时发现

黄赌毒,指卖淫嫖娼,贩卖或者传播黄色信息、赌博、种植，买卖或吸食毒品的违法犯罪现象。在中国,黄赌毒是法律严令禁止的活动,是政府主要打击的对象。所以要即将发生及对发生的 该事件进行上报。

9.29 邪教组织及时发现

一些极端教派一意孤行,奉行反社会、反文明的教义,实施教主极权统治,对信徒强制洗脑和精神控制,摧残人权,危害社会,成为具有严重犯罪性质的极端恶种——邪教组织。所以要即将发生及对发生的该事件进行上报。

9.30 公共设施管理

公共设施是由政府提供的属于社会的给公众享用或使用的公共物品或设备。按经济学的说法,公共设施是公共政府提供的公共产品。从社会学来讲,公共设施是满足人们公共需求(如便利、安全、参与） 和公共空间选择的设施,如公共行政设施、公共信息设施、公共卫生设施、公共体育设施、公共文化设施、公共交通设施、公共教育设施、公共绿化设施、公共屋等。我们通过对 XXX 区社区内设备登记,及时发现公共设施问题,以便进行实时的更新,以达到便民的效果。

9.31 志愿者管理

志愿者指在不为任何物质报酬的情况下,能够主动承担社会责任并且奉献个人的时间及精神的人。我们通过志愿者管理对希望成为志愿者及已经是志愿者的人进行管理。对一个需要志愿者去做的是可以以短信和邮件的形式进行通知。可以更好的运用人力资源。

第十章 社会化治安防控力量实战指挥

10.1 指挥调度及警令流程

此功能是派出所、分局针对警情处置、应急突发事件处置、专项行动任务部署,利用智工业园区社会综合治理云平台指挥调动社会服务管理对象（警务助理、信息员、社会巡防人员） 进行参与辅助。系统依托互联网与物联网 ， 集成 GIS、PTT、4G 对讲等技术 ， 通过“地理位置标注” ， 可以在电子地图上对各保安单位值班岗点实现直观显示 ， 还可以通过 “定位跟踪” 功能 ， 对安保人员的值守及工作情况进行实时掌控； 平台“对讲群呼” “ 急框选呼叫” 则可实现辖区内的安保力量的 急调集 ， 协助公安民警处置 急突发事件； 实现警民联动的综合指挥调度,分区域、分时段、分作战单元部署任务。一次重大事件的多个作战单元,各自生成临时通信组,组内成员可以以语音、文字、图片、视频等方式进行信息共享,组内其它成员可以同步看到,从而达到协同作战、保障作战的目的。派出所、分局的勤务指挥中心能够了解到各作战单元各力量的情况（位置、状态、事件进展） ,可以一键呼叫、视频回传、发送信息公告等。

10.2 智能堵控圈

知据犯罪嫌疑人逃跑的方式,依据不同时间点（例：5 分钟、1 5 分钟、30 分钟） ,将预先设定治安岗亭、道路卡口,自动生成三道堵控圈,系统自动分析其周边服务管理对象资源,以互联网 APP 端通知指令或语音方式发给相关人员,让其前往协助堵截抓捕,从而提高抓捕犯罪嫌疑人速度,织就一张社会治安防控的安全大网。

10.3 一键“关城门”

派出所、分局的勤务指挥人员启用“一键式” 布控按钮,相应的基层值班室的电脑终端和卡点职守民警、社会化巡防人员的智能终端上同时收到上岗指令。民警及社会化巡防人员接到指令后赶往各自堵控点。当有警力到达堵控点后,红色堵控点图标自动显示绿颜色。勤务指挥中心可以通过布控查勤,对各个布控点警力到岗情况进行查阅。

10.4 指挥过程全流程管理

智工业园区社会综合治理云平台在整个的指挥调度过程中会对指挥调度人员的所有操作进行记录,包括指挥过程、案件信息、指挥中的录音、指挥中调用的周边资源、视频资源等,同时对这些记录的信息提供信息检索、统计分析、导出等操作。实现指挥全流程的监管。

10.5 总体架构

知 XX 区社区综合信息服务平台架构分为接口平台、服务层、数据层和感知层四部分,接口平台可以独立建设并挂载在 xx 智能城市平台的服务接口上,作为子接口(页面),也可以直接使用 xx 智能城市平台的服务接口,将各个平台作为功能模块建设。

权限管理模块用于在用户登录时鉴别用户所属的角色,各子平台通过角色划分操作和管理权限,根据角色决定其使用功能及数据查看权限。XXX 区社区综合信息服务平台的接口平台、服务层和数据层部署在 xx 智能城市云平台上,通过数据中心的虚拟化云服务来提供运行资源,并通过智能城市(有线和无线) 网络与感知层和用户进行连接。

感知层包括 XXX 区社区、医疗等服务所使用的各种前端监控、感知设备,监控类设备建设在 XXX 区社区范围内,由物业公司进行使用和维护,上报的信息直接存入 XXX 区社区信息数据库中供各平台使用,医疗腕带等健康管理设备由医院为 XXX 区社区高龄老人发放,对其健康和位置信息进行监控,信息直接存储在 XXX 区社区信息数据库中。智能水表、电表等感知终端通过智能城市无线网络定期将住户的使用情况上报供水、供电等公司,在由各公司将信息同步到物业服务平台。物业公司和 XXX 区社区为工作人员发放工作终端,终端随工作人员的走访巡逻采集信息并存储在 XXX 区社区信息库中,工作终端需要在采集信息的同时作为工作人员访问使用各类 XXX 区社区综合信息服务平台的渠道

10.6 XXX 区社区信息数据库

XXX 区社区信息数据库作为 XXX 区社区综合信息服务平台及各子平台使用的统一标准数据库,对 XXX 区社区综合信息服务相关的各类信息进行分类存储,供各平台实时调用,XXX 区社区信息数据库对各类数据进行逻辑划分.

用户信息根据权限区分 XXX 区社区综合信息服务平台的各类使用角色,配合权限管理模块实现分级、分权限用户管控。服务和审批流程信息库则存储全部园区审批和 XXX 区社区、物业服务请求的详细受理情况,以此实现对 XXX 区社区网格化管理服务平台提供的各类服务的流程化受理、监管和查询。商务和公共信息库则存储需要对民众发布宣传的各类政务信息和政务办理流程说明,同时为信息发布平台进行 XXX 区社区政务公开服务。商务和公共信息库存储 XXX 区社区便利店和家政等网上便民服务的信息,为商务缴费平台服务,同时接收水电热气公司同步的住户使用情况,用以实现网上查询和缴费。

人口、医疗、社保、救助等信息通过 XXX 区社区综合信息服务平台和各平台实时更新,并根据市镇管理部门的要求,定期向智能城市基础数据库(四库) 同步信息。监控信息可根据需要与公安、交管等部门共享。

10.7 信息数据管理平台

信息数据管理平台作为 XXX 区社区、镇、市工作人员录入和查询信息的统一接口,建设目的在于解决目前 XXX 区社区垂管信息平台过多导致的使用困难,如信息的重复录入、不同平台登录方式,身份密钥不同、网络原因导致连接中断,信息录入效率低等问题。同时解决因信息分散存储在不同的垂管平台上引发的查询汇总困难。

xxXXX 区社区、镇、各园区机关目前使用的信息化平台,都是由州、自治区里不同的垂管部门开发并开放给市镇使用的,目前 XXX 区社区和镇方面使用警综平台、流动人口管理平台、xx 州 XXX 区社区网格化管理服务平台平台、卫生计生平台和保障性住房管理平台； 园区局使用低保人员救助平台、医疗救助平台、流浪乞讨人员救助平台、残疾人就业需求保障平台、婚姻登记平台和救灾报灾平台； 卫计、医院和人社局使用公共卫生管理平台和金保工程平台。其中以 XXX 区社区使用的平台最为庞杂,不同垂管部门对数据上报都有完善的要求,导致人口基本信息需要反复上报。

信息数据管理平台将各垂管平台需要录入上报的数据信息汇总合并成并集存储在 XXX 区社区信息数据库中,工作人员在填报时只需要对该“并集” 进行一次录入操作,信息数据管理平台会自动抽取各垂管平台需要录入的数据,定期、自动完成录入。

平台将各垂管平台的共同数据（基础信息数据） 抽取出来，并结合各垂管平台的专有业务信息存储在 XXX 区社区信息数据库,工作人员在走访调研后,只需通过信息数据管理平台进行一次录入,即可将调研获取的全部信息保存在 xxXXX 区社区网格化管理服务平台综合信息服务平台中,工作人员和园区主管部门需要查询数据时直接访问 XXX 区社区信息数据库即可查询到所有信息。

信息数据管理平台定期将各垂管平台需要上报的相关信息组合,并录入进各垂管平台,该过程由信息数据管理平台自动完成,不需要 XXX 区社区工作人员手动参与。信息数据管理平台建设在智能城市云平台上,园区工作人员通过本地网络访问使用,避免因网络问题导致远程访问垂管平台的数据时出现掉线、断线等情况使信息录入无效。信息数据管理平台为每位园区工作人员设置独立的登录身份,避免使用垂管平台时因“多人一号” 导致的使用冲突,而提升工作效率。

10.8 物业管理平台

物业管理平台的建设目标：实现物业公司对 XXX 区社区监控、绿化等设施的和安防的自动管理；实现物业公司对居民物业诉求的电子化流程受理； 实现物业费用的收缴； 实现 XXX 区社区、

镇园区管理部门对物业公司的考评和管理。

根据建设目标将物业管理平台分为物业管理模块和物业服务模块。

（1） 物业管理模块

物业管理模块对居民区内的监控、巡更、车辆等管理方面使用的智能设备进行控制,辅助物业公司实现对居住区情况的掌控和维护 XXX 区社区治安,通过门禁、烟雾感知等终端实现对非法入侵和消防灾情等的实时感知和告警。

为实现维稳和安防要求,保障小区治安,需要在小区内各楼宇、公共休闲场所设置监控和门禁平台,XXX 区社区安防监控设备通过无线的方式就近连接小区单元内的无线交换设备,并同小区单元内的门禁、烟感等设备一同受小区单元内的管理设备所控制,交换、管理设备接入传输网络,并最终接入建设在 xx 中心的云数据中心,xx 的智能城市传输网络采用租用运营商带宽、管口的方式建设。车辆、停车管理和电子巡更平台则通过物业公司的办公室连接物业管理平台。

前端感知设备默认将监控、采集的信息存储在 XXX 区社区信息数据库中,物业公司和 xx 园区部门通过物业管理模块实现监控信息的实时调取,实现对门禁、IPC 等设备的远程管理。当烟感、门禁等设备遭到破坏或检测到突发事件时,物业管理模块会发送告警,通过智能城市统一接口平台将告警传送到指挥中心或工作人员的工作终端、手机 APP,实现告警推送。

物业管理模块对维护 XXX 区社区安防,维稳具有重要意义， 消息预警模块可通过大数据分析技术和人脸识别技术,自动对 XXX 区社区信息数据库中监控设备采集到的影像进行分析,实现罪犯识别,并对非法闯入等现象实时报警。

（2） 物业服务模块

物业服务的主要对外工作即受理居民业主的各种请求、物业费用的收缴及提供公共服务。业主或住户的请求主要包括设备报修、绿化清洁、车位申请及小区治安管理等。公共服务则包括定期巡视、清洁、设备检修、停车费用收取等。物业公司在物业服务受理行动中的效率、态度和完成情况直接影响业主和住户的感受。

同时,园区部门或物业管理机构需要通过物业公司的工作执行情况和物业请求的办结情况对物业公司进行考核,或根据上述信息调查处理居民对物业公司的投诉。

物业服务模块通过电子流程 （工作流） 的方式将业主住户的诉求、物业公司的接收处理、工作受理进度及受理时间等在信息平台中显示并归档。通过该方式使物业公司在服务受理方面有据可循,有理可循,即避免了物业公司在受理诉求时推脱不行动、也解决了由居民恶意举报为物业公司带来的损失。政府工作人员通过该模块可定期对物业公司的工作记录进行查询监督,完成对物业公司的考评和打分。

物业服务模块根据使用者的不同提供不同的服务，物业服务模块禁止私人注册,业主及租户的信息应由本人联系物业公司报备后录入,物业公司可查询业主、租户的物业费缴纳情况,并通过该平台对其进行通知,业主、租户尽被允许对登录密码进行更改,其他信息的更改需联系物业公司进行。

居民（业主、租户） 使用物业服务的主要目的是提交物业服务申请、缴纳物业费及查询申请的受理情况。物业服务平台将申请电子流程化并令其在各执行阶段清晰可见,居民通过物业服务模块提交申请,非投诉类申请提交物业公司,物业公司根据内容的不同,将服务申请分发给下属工作人员或

第三方合作公司受理,受理人员在受理接收派出,和处理完结后更新工作流程,并提交物业公司确认,最终提交申请者 （居民）确认办结。申请的整个过程都在信息平台中通过流程化显示,居民在任意时刻都可以通过物业服务模块查询自己申请的办理进展。处理进展在平台中会以类似于京东购物 -派送流程的方式显示,令查询者（居民、物业公司、园区机关） 一目了然。

通过权限管理,居民在物业服务模块中仅能对自身提交的申请进行查询,物业公司的服务、工作人员及合作第三方可查看所有经其处理的申请的全流程,制定定时巡查计划

物业公司

物业服务模块

定时调度 、提醒巡视、巡逻清洁清扫

巡检维修

保安

绿化环卫人员

维修检修人员

巡检记录 、工作记录

物业服务模块确认 、统计、归档

物业公司定期巡检是物业公司服务工作中的重要一环,该流程不需要居民参与,面对物业公司,定期巡检管理和执行工作中最困难的当属员工的考勤和监管工作,物业管理平台通过集成工作终端、电子巡更等方式实现对员工巡检工作的监管和跟踪。

物业公司制定巡检计划并指定巡检责任人后、服务模块会在巡检执行前自动通知对应任务的责任人,并由责任人下发任务、组织巡视（检） ，巡检过程中员工的巡视轨迹通过巡更平台上报,员工在发现问题时通过工作终端拍照并录入巡检记录。物业服务模块会将上述信息归档存储,便于物业公司和监管部门查询。物业公司通过归档的巡检和工作信息确认员工的工作和绩效评定。

物业管理平台的工作信息流,经录入确认后,仅授权管理维护员(政府信息中心工作人员）更改,管理平台的使用者 （居民、物业公司、第三方公司、园区部门） 无权修改工作流程、记录等信息,通过该方式、平台确保相关信息的可靠性和可追溯性。

10.9 园区服务审批平台

目前在 xx 市居民申请低保救助、暂住居住证、保障性住房、申请社会奖励、结婚生育登记等的第一渠道都是 XXX 区社区,再通过 XXX 区社区人员指导去对应的职能部门办理,园区服务审批平台为居民申请提供统一的接口。居民的各类园区行政申请通过平台统一提交给 XXX 区社区,再由 XXX 区社区根据类别提交到各园区职能部门。

上述申请的最终审批权在政府各职能部门、XXX 区社区和镇在审批流程中仅起到转发和辅助审批的作用,审批的发起 - 办理 -办结各环节的关系部门与行政服务审批相似,因此建议园区服务审批作为行政服务审批平台的一个子流程建设,不再单独作为子平台建设,以此方式实现政务审批平台

的统一化。

区审批功能在电子政务平台的行政审批模块一并实现。居民在提交园区审批申请后,会统一由XXX区社区进行受理、初审,在初审确认后,XXX区社区将用作初审评判的材料和信息一并提交职能部门,职能部门在最终审核时无需再向 XXX区社区、镇一级要求数据。在低保、救济、保障性住房等申请过程中,镇一级无需再进行复查安排,只需做到备案监督即可。最后阶段的审核和复查由园区局完成。

10.10 XXX区社区商务缴费平台

商务缴费平台的建设目标是提供一个供 XXX 区社区居民缴纳水电煤等生活费用,以及在XXX区社区内部买卖、交易、进行商务交流的平台。根据 xx 目前的状况和发展目标,优先进行水、电、燃气、供暖等集中缴费的建设。

集中缴费终端

xx 目前的发展规模较小,XXX区社区数量少且相距较近,因此除电业公司外,供水、采暖、燃气等公司尚未实施线上缴费，供水公司建设成水卡缴费平台,但目前只在供水公司大厅设有缴费终端。通过联合水、电、燃热公司和银行机构,建设自助查询- 缴费平台,并部署在缴费终端上,居民可以在小区内实现对上述生活用度的查询和缴费。

自助缴费平台通过与供水、电、燃热等公司的接口,实现居民（业主） 对各类使用费用的查询;通过与银行的借口实现使用银行卡自助缴费,自助缴费平台部署在市区内各缴费终端上,居民使用小区内的终端即可实现就近缴费。

XXX区社区商务平台的功能框架,其中包含部署在缴费终端的自助缴费子平台,盖子平台与部署在缴费终端的版本唯一的区别即缴费方式由读取银行卡变为线上支付,支持网银、支付宝、微信等主流交易方式。XXX区社区商务子平台则 XXX区社区内居民提供商品交易,家政服务等的线上平台,通过网上商城的方式为居民提供各种生活服务。

水、电、燃热无线抄表改造

xx 市各小区的建设实践跨度大,设施新旧程度也不统一，对工作人员上门查表记录带来很大困难,需要对各类水表、电表等设施进行无线化改造。因 XXX区社区缴费平台的建设和使用与各类生活资源读表相独立（居民查询直接通过资源公司的平台，各资源公司统计用量时读表并录入平台,两过程相互独立,互不影响） 。则水、电、燃热抄表的改造可逐户逐步进行。

智能表通过自带的无线模块和运营商提供的定制 sim 卡接入运营商网络,接入后智能表会连接资源公司的服务器,并定时自动上报读数,资源公司的服务器在接到上报后将读数存储在智能表对应的业主信息库里,供查询、缴纳核算等工作使用。

10.11 医疗服务平台

医疗服务平台为居民提供信息化的健康管理和养老服务,通过为老年人发放智能腕带对其健康状况进行管理、提供定位服务,人民医院通过医疗服务平台管理居民的健康档案,对其身体健康情况进行了解并提供针对性的健康服务,通过健康档案管理,对居民进行体检、疫苗接种、防疫等在线提醒,提供医疗服务。医疗服务平台通过基础信息库或电子政务平台信息库获取民众的医保社保信息,供居民查询。

健康检测腕带能够对温度、血氧饱和度、脉搏及佩带者自身所处环境状况等信息进行查询。对于老人、病人这类依赖人们照顾的群体,当健康腕带检测到健康信息或者环境信息异常时,腕带会对医疗服务平台实时上报告警,并由平台通知医院 （公共卫生科） 、XXX 区社区及老人、病人的家属,避免意外的发生。腕带同时带有 GPS 定位模块,当家属发现老人走失时,可通过医疗服务平台确定老人目前的位置,以最优的效率完成找寻。医疗服务平台拥有统计报表功能,可以将老人、病人近一段时间的身体状况生成报表呈现给家属和医院,辅助家属及医疗机构完成对老人、病人的健康管理。健康检测腕带带有 3/4G 模块,通过内置的 sim 卡片接入运营商电信网络,实现对佩带者信息的远程上报,无需佩带者再行配置蓝牙或移动终端。医疗服务平台对 XXX 区社区居民建立健康档案,医院(公共卫生科） 通过将健康档案对居民的身体状况进行了解,并和电子病历平台进行联通,在居民就医时实时查询其最近的健康状况,辅助诊断。XXX 区社区和医院也可通过医疗服务平台对需要体检、注射疫苗的居民 （儿童）进行通知。健康档案和健康管里可通过有偿服务的方式来供居民购买使用。

10.12 信息发布平台

信息发布平台面向 XXX 区社区居民,实现宣传和政务公开等功能。居民从信息发布平台中了解到镇、市的各项最新政策方针， 规定,通报等。XXX 区社区、镇园区方面的考评、选举、办结率等信息也通过该平台对居民公布。信息发布平台还为居民提供园区、行政审批的办理流程、材料准备等指导和帮助。对各项物业申请的办理周期,响应周期也可通过该平台向居民公开,使居民的各项申诉投诉有据可依,有理可循。

XXX 区社区网格化管理服务平台平台的信息发布不应单独建设,而是应与城市管理、电子政务(行政园区审批） 等平台的对公众信息发布公用一套平台,可在 xx 智能城市统一接口平台下作为单独的页面/模块来实现,将该页面/模块作为城市信息发布的统一接口。

10.13 园区管理平台

人口增长、流动人口信息、老龄化信息、出生率、XXX 区社区入住率,以上等等信息都是政府部门领导对城市管理、建设发展等进行规划,编制年鉴,进行工作上报时需要获取,汇总的信息,依托于智能城市和 XXX 区社区网格化管理服务平台平台,政府管理人员可以直接对 XXX 区社区统计编辑的

信息进行读取,但读取出的原始信息仍需要政府部门进行加工、分析、生成报表后才能发挥作用。

园区管理平台帮助政府工作人员完成上述工作,对 XXX 区社区信息数据库里存储的原始数据进行分析、归类,绘图并生成报表。同时按照政务部门的要求生成园区数据类的汇报表格,使其可以直接用于政府工作报告中。

园区管理平台通过使用大数据分析技术,对 XXX 区社区采集到的各类人口信息进行分析,并结合历史数据生成人口发展曲线、流动人口曲线,辅助政府管理人员对 xx 市的后续发展、变更做出规划和指导。园区管理平台对使用者进行严格的权限控制,群众、物业公司和 XXX 区社区工作人员等没有权限使用,镇级管理者能够对 XXX 区社区一级人员的工作进行查询和监管,市级管理者有权对 XXX 区社区和镇一级人员的工作进行监管。通过该平台管理者可对下一级员工的绩效和考评进行打分评价。

第十一章 园区管理平台

11.1 勤务资源库管理

呃呃

11.1 勤务资源库管理

呃呃

11.1 勤务资源库管理

呃呃

11.1 勤务资源库管理

呃呃

11.1 勤务资源库管理

呃呃

11.1 勤务资源库管理

呃呃

11.1 勤务资源库管理

呃呃

11.1 勤务资源库管理

呃呃

11.1 勤务资源库管理

勤务资源库是针对智工业园区服务管理对象（警务助理、信息员、社会化巡防人员） 这些成员及组织机构、单位进行统一管理,勤务资源包括人员、通信设备、车辆等。以及人员与通信设备的绑定关系。呃

11.2 值班备勤

实现对智工业园区服务管理对象（警务助理、信息员、社会化巡防人员） 每日值班、备勤信息的录入、编辑、展示以及向上级单位汇聚的功能。

11.3 巡防报备

主要是针对勤务的巡防区域在图上进行设定,包括日常巡逻区域管理、重点观测点管理等。设置内容包括勤务时段、勤务类型、任务、上岗区域、组织单位、人员、通信设备以及勤务规则管理。

11.4 专项任务勤务报备

主要包括专项行动、卫防护、要害保卫、治安隐患排查等。主要是针对任务进行任务类型、任务名称、地图区域、人员安排、任务管理等。根据任务复杂程度可设定多个子任务 （子任务内容、时间、地图区域、警力、勤务规则） 支持任务报备的流转。

11.5 勤务查询

查询中,可以对所有的勤务工作进行查询,可根据日、周、月 对所属辖区的所有勤务进行日历展现,并支持按勤务类型或人员进行筛选。

在智工业园区民警互联网 APP 端和 PC 端,对当前辖区出勤人员、备勤人员、各自任务、巡区划定等信息进行统计查询。

11.6 勤务监督

勤务督查主要是对报备的勤务信息进行监控,查看是否出现违规现象。勤务督查主要包括：人员监控、轨迹回放、越界报警、超长停留报警、离线报警等。

人员监控：针对每个巡区,对其人员到岗情况进行实时监控，

如果在该岗点周围一定范围内 （可配置） 有指定的任何一个互联网智能终端即为到岗,岗点图

片显示绿色,如果该岗点周围指定范围内没有任何指定的智能终端,岗点图片显示红色。

越界报警：根据事前制定的报备预案,系统对报备的智能终端都分配固定的巡逻区域和执勤规则,巡逻人员若是在值勤时间内超出自己的巡逻范围,系统报警提示及自动保存违规记录,为该人员的绩效评估做依据。

超长停留报警：根据事前制定的报备预案,系统对报备的智能终端都分配固定的巡逻区域和执勤规则,在值勤时间内长时间定制不动,系统报警提示及自动保存违规记录,为该人员的绩效评估做依据。

离线报警：根据事前制定的报备预案,系统对报备的智能终端都分配固定的巡逻区域和执勤规则,报备的智能终端在值勤时间内出现离线或掉线情况,系统自动保存记录,为该人员的绩效评估做依据。

轨迹回放：根据指定管辖范围内的人员以及执勤行动的时间段,用户可以实现对指定人员历史轨迹的查看及动态回放。智工业园区可以根据历史轨迹可以确定人员在上班时间是否离岗； 应急调度时可以了解人员当前的轨迹以便勤务指挥中心民警决策。

11.7 绩效统计

可针对个人、单位提供信息提报、值班备勤、巡防报备、专项任务的效果评估,通过一定的算法给出执行任务次数、执行任务时间、信息上报次数、上报质量、警民联动次数、违规统计等。

第十二章 服务管理对象互联网 APP

12.1 治安防控信息上报

上报方式是在管理服务对象的移动终端安装 APP,服务管理对象在该 APP 的管理下采集提报信息,这些信息包括但不限于社情民意搜集、矛盾纠纷排查调解、案件线索、非法集资/非法集会 /吸毒涉黄信息、治安隐患点、违法犯罪行为、警情等。

APP 上报

信息以点对点方式发送给上级智工业园区民警,确保信息安全不被泄露,同时会关联上报人员坐标信息,通过消息方式传送至智工业园区社会综合治理云平台在地图上显示。同时通过数据库服务方式将上报详细信息推送至平台数据库中,在地图上的气泡框中可点击查看信息详请。

12.2 我的上报历史信息

服务管理对象 APP 能够查看自己报送的信息并查看智工业园区民警反馈。能对报送信息进行信息追加、更新

12.3 我的任务

可以按天、星期、月 展示智工业园区民警分配给服务管理对象的所有任务,包括值班任务、巡防任务、专项任务等,点击某个任务可以查看任务详情,包括任务时间、工作区域、团队成员、工作内容等,可及时反馈任务处置状态及现场情况。

12.4 工作任务反馈录入

智工业园区民警在系统设置任务部署,如专项任务,当服务管理对象在现场处置完,通过 APP 对处理信息进行反馈； 支持文字、图片、视频、语音等方式的录入。

如超过规定时间,系统会有提醒,超过一定时间,则在系统中进入异常提醒,以便智工业园区民警进行专项监督；

12.5 警务即时通信

智能终端用户之间可以进行即时消息通信,支持文字、图片、语音、视频等格式的消息。支持一对一沟通和任务群组沟通,也可以支持用户自行创建群聊组。

12.6 警务通讯录

根据组织机构显示智工业园区民警、派出所民警、服务管理对象通信录，点击人员获取详细信息，可一键发起语音、视频、短信通信。

12.7 现场取证多媒体资料回传

服务管理对象在日常巡逻、守卫防护、要害保卫、治安隐患和问题排查处理过程中可以进行现场的取证和及时的多媒体反馈，在网络情况不好，实现断点续传。服务管理对象可以以文字、图片、视频的形式把现场及相关情况及时的反馈到智工业园区社会综合治理云平台中，为派出所民警制定下一步工作安排做出支撑和参考。

12.8 一键报警

服务管理对象可对现场巡逻、执勤发现的警情，进行一键式快速上报。自动上报智能终端所在地点坐标、上报服务器自动生成警单。

12.9 通知公告

实现对用户进行组织内部消息、工作消息进行告知，可支持对上级单位下发的重要通知、会议通知、日常工作通知、重大任务通知等功能。

12.10 审批

可以发起调班、调换携带的通信设备申请

12.11 勤务数据分析

可以按月、季度、年度统计个人的各项勤务数据，如信息提报次数、有价值信息次数、值班工作量、巡防工作量、专项任务参与次数、参加警民联动行动的次数，以及违规次数。

第十三章 智慧工业园区云平台建设

13.1 总体建设方案

13.1.1 智慧园区大数据云总体架构

结合前期调研和 XX 市政府实际需求,智慧园区大数据云平台总体架构规划包括当前数据中心,同城 A、B 两个数据中心以及一个异地灾备中心。每个中心的定位如下：

同城 A、B 数据中心：两个生产中心共同承载 XX 市智慧园区大数据云平台,同时,将政府业务应用系统分别部署在 A、B 两个数据中心； 其中关键应用在 A、B 两个数据中心间实现互为备份,从而提高 XX 市智慧园区大数据云的业务连续性。

异地灾备中心：同时为运行 A、B 两个数据中心中的业务应用系统提供异地数据容灾备份。

XX 市政府当前数据中心：当前数据中心为各局委办汇聚点,是政务网的汇聚中心； 同时 续承载一些政府的暂时无法迁移到智慧园区大数据云上的业务应用系统； 还承载着智慧园区大数据云监管平台的功能,对各个云服务商进行统一的监管,主要实现宏观调度、资源申请、监控、审计等功能。所以,当 XX 市智慧园区大数据云建设完成启动运营后,当前数据中心将作为 XX 市电子政务网络汇聚中心、存量业务数据中心和智慧园区大数据云监管中心 续运行。

13.1.2 数据中心间互联架构

1） 在当前数据中心、A 数据中心和 B 数据中心中分别部署一套密集型光波复用（DWD）M 设备,并为每套密集型光波复用（DWD）M 设备配置万兆接口卡,同时在密集型光波复用（DWD）M 设备之间通过 2 对裸光纤进行互联,从而实现当前数据中心、A 数据中心和 B 数据中心三个数据中心间实现高速连接,满足业务访问需求。

2） 密集型光波复用 （DWD）M 设备通过多路复用一对光纤载波的密光谱间距,提供多条 路,用于实现各中心之间广域网、局域网、管理网、存储网的互联。

3） A、B 两个数据中心与异地灾备中心通过千兆以太网线路互联，为业务数据的异地容灾备份提供数据传输通道。

为保证三中心之间的业务稳定可靠运行,需要满足以下要求：

1）距离：现有中心和 A、B 两个数据中心是同城数据中心,为了保证多中心间网络的稳定性及业务系统的高可用性,三个中心相互之间的距离建议不要超过 30 公里（此距离是光纤 路距离） ,如果超过 30 公里,最大距离建议不超过 50 公里。因为超过 30 公里后,会因为光纤质量问题和距离问题,需要增加光波放大器,随着距离的不断增加,放大器的数量也会增加,造成成本增加的同时,也增加的网络的不稳定性因素。

2）光纤要求：远距离传输,必须是单模光纤,为了保证稳定性，需要提供 2 对裸光纤,并要求 2 对裸光纤在不同的管道井中，并且这两个管道井相隔距离建议大于 1 公里。

3）延时要求：推荐 5 毫秒以内,最大不得超过 1 0 毫秒。

13.1.3 云服务商平台总体架构

XX 市智慧园区大数据云云服务商平台总体架构：

1） XX 市智慧园区大数据云云服务商平台整体建设分为两部分，包含新建 xxx 网云平台、新建互联网云平台,为政府各级单位信息化建设统一提供基础设施支撑。xxx 网云平台承载政府各局委办的自有业务应用系统,包括新建和改造业务系统； 互联网云平台承担面向社会公众服务的内容,如政府网站统一门户等；

2） xxx 网云平台与互联网云平台之间物理隔离,通过部署网闸实现严格受控的数据访问和网络互通。针对云平台的安全防护,xxx 网云平台在出口部署云安全访问控制区,互联网云平台在互联网出口部署云安全访问防护区。各局委办单位通过云安全访问控制区访问政务外网云平台,通过互联网云安全访问防护区访问统一门户网站和对公众应用；

3） 从部署架构上看 XX 市智慧园区大数据云是两个云平台,但是为智慧园区大数据云的客户提供的是统一的自助服务门户平台,客户可以通过这一个门户系统分别申请两个数据中心,分属于不同业务区域（xxx 网业务区和互联网业务区） 的云服务；

4）两个云服务商平台之间可以实现关键业务的互备,同时将所有业务数据备份到异地容灾中心；

5） 两个云服务商平台都有自身的互联网出口。

13.1.4 智慧园区大数据云总体网络拓扑设计

13.1.4.1 现有数据中心改造

委办局连接：当前在 XX 市所有委办局单位当中,与 XX 市政府当前数据中心连接方式有以下两种：

1 ） 一部分委办局的办公局域网网络设备直接连接到当前数据中心核心交换设备,通过内部网络直接访问当前数据中心业务系统。

2）另外一部分委办局需要通过广域网接入到当前数据中心核心交换设备,通过广域网访问当前数据中心业务系统。

政府当前数据中心未来定位：

未来所有委办局和政府当前数据中心的连接方式不变，政府当前数据中心将作为未来所有委办局访问 XX 市政府云统一网络出口。

关键点：

1） 通过如上需求的分析,政府当前数据中心核心设备 S9512E 将承载未来 XX 市智慧园区大数据云业务管理和访问统一出口。如果 S951 2E 出现任何故障,都将造成所有委办局无法访问智慧园区大数据云平台以及业务系统。

2） S9512E 需要通过万兆光纤与智慧园区大数据云进行连接。从可高性角度初步分析,每台 S9512E 至少需要 2 个万兆接口。S951 2E 情况介绍：

1 ） 采购时间为 ***0 年,到目前运行时间为 6 年,

2） 万兆接口没有剩余接口可用；

3） 无法进行板卡升级或者通过新增板卡进行扩展

4） 此设备当前已经停产。

政府数据中心核心规划：

基于以上几点需求分析,政府当前数据中心核心规划如下：

所有的连接方式不变,用新的 S1 051 0 替换 S951 2E。

XXX S1 0500 系列交换机产品是 XXX 面向下一代园区网核心设计开发的核心交换产品。

1） 采用先进的 CLOS 多级多平面交换架构,可以提供持续的带宽升级能力 .

2） 支持数据中心大二层技术 TRILL、纵向虚拟化和 MD（C 一虚多）技术,支持 EVB 和 FCOE，并完全兼容 40GE 和 1 00GE 以太网标准。

3） 该产品基于 XXX 自主知识产权的 Comware V5/V7 操作系统，以 IRF2、IRF3 技术为系统基石的虚拟化软件系统,进一步融合 MPLSVPN、IPv6 、应用安全、应用优化,等多种网络业务,提供不间断转发、不间断升级、优雅重启、环网保护等多种高可靠技术,在提高用户生产效率的同时,保证了网络最大正常运行时间。

13.1.4.2 现有数据中心、A 中心和 B 中心连接设计

以 xxx 网为例,物理连接图如上所示,现有数据中心、A 中心和 B 中心之间的物理连接。

基于以下安全合规性、可管理性、高稳定性以及可扩展性要求，将云中心内部网络划分为管理网、局域网、SAN 网络。

a) 安全合规性：

先关安全标准要求管理网络和业务网络要实现有效隔离,禁止通过业务网络捕获管理流量,在业务区、公共业务区（即：xxx 网） 和

互联网业务区间可以共用一套管理网络； 智慧园区大数据云中部门业务区、公共业务区（即：xxx 网） 和互联网业务区（互联网） 间业务网络实现有效的安全隔离； 业务区、公共业务区（即：xxx 网） 和互联网业务区间可以共用一套存储系统。

从上述的描述中可以看出,在智慧园区大数据云建设和运行中，安全和稳定是第一位要确保的内容,为了保证智慧园区大数据云的安全、稳定和高效运行,网络最佳建设方案是划分管理网络、业务

网络（局域网） 和存储网络（SAN 网络） 。

b） 可管理性：

这样的划分可以对负载的网络化繁为简,从而提高可管理性。

c） 高稳定性：

三网分离,可以有效提高网络系统整体的高稳定性,并不会随着整体网络系统的扩展而降低。

d） 可扩展性：

未来智慧园区大数据云平台会随着业务的不断增加而变得越来越大,如果将管理网络、业务网络和存储网络分离,从整体架构上可以有效提高智慧园区大数据云整体的扩展性和可持续的管理性。

广域网互联：

对于 xxx 网,现有数据中心、A 中心和 B 中心之间双线互联； 对于互联网情况相同。

局域网互联：

对于 xxx 网,A 中心和 B 中心之间双线互联； 对于互联网情况相同。

管理网互联：

对于 xxx 网,现有数据中心、A 中心和 B 中心之间双线互联； 对于互联网情况相同。

存储网互联：

A、B 中心 xxx 网和互联网共用存储网络,A 中心和 B 中心之间双线互联。

其中原数据中心侧的两个波分设备,用于与云中心 xxx 网广域网、管理网,与云中心互联网广域网、管理网,需要将波分拆分为 8 条线路。

A 云中心的两个波分设备,除了用于与原数据中心 xxx 网广域网、管理网互联（各两条线路） ,与原数据中心互联网广域网、管理网互联（各两条线路） ,需要实现两个云中心之间的 xxx 网云中广域网、局域网、管理网、存储网的互联（各需 4 条线） ,还需要实现两个云中心之间的互联网云中广域网、局域网、管理网、存储网的互联（各需 3 条线,其中存储 xxx 网与广域网公用） ,共需 11 条线。

同样的 B 云中心的两个波分设备也需 11 条线。

13.1.5.1 xxx 网安全拓扑设计

xxx 网安全组网拓扑广域网出口配置了一对 VPN 设备， 允许特定人员通过互联网拨入,实现远程移动办公。另外出口配置了两台 M9000,除了具备防火墙的功能,还具备 IPS 功能,实现原数据中心与云生产中心之间的安全防护。

数据库系统区配置了一套数据库审计系统,对数据库操作进行审计。

东西向安全资源池中包含 vFW 和 vLB,为租户提供 fw 及负载均衡服务。

云管理区配置堡垒机、漏洞扫描（含 WE 漏 B 扫、数据库漏扫、系统漏扫） 、安全管理中心各一套。

另外,在每台服务器上部署亚信杀毒软件,实现对服务器的安全防护。

13.1.5.2 互联网安全拓扑设计

互联网安全组网除配置与 xxx 网相同的 FW、IPS、SSL VPN、数据库审计、堡垒机、漏洞扫描、安全管理中心,杀毒软件,以及安全资源池的 vFW、vLB,另外配置了 DDoS （第三方设备） 、行为审计、网页防篡改、WAF 、硬件负载均衡、安全管理检测中心等。

一套 DDoS 设备和两台行为审计设备部署在广域网出口。网页防篡改部属在各应用服务器上。

WAF 和硬件负载均衡设备旁挂核心交换机,部属在核心交换区安全管理检测中心部属在云管理区。

13.1.6 云管理平台架构设计

13.1.6.1 IT 架构面临的问题

1） 传统 IT 面临的困境

近几年云计算在全球范围内得到了迅猛的发展,IT 基础架构平台的规模和复杂程度出现了大幅度的提升,与此同时,很多政府单位的数据中心却因为这种提升而面临着新的困境。

高昂的成本支出和管理运营成本。

数据中心内的服务器数量、网络复杂程度以及存储容量急剧增长,随之带来的是高昂的硬件成本支出以及运营成本支出 （包括电力、制冷、占地空间、管理人员等） 。

缓慢的业务部署速度。

新的服务器、存储设备和网络设备的部署周期较长,整个过程包括硬件选型、采购、上架安装、操作系统安装、应用软件安装、网络配置等。一般情况下,这个过程需要的工作量在 20～40 小时,交付周期为 4～ 6 周。

分散的管理策略。

数据中心内的 IT 基础设施处于分散的管理状态,管理员遵循 “根据最坏情况下的工作负载来确定所有服务器的配置” 这一策略导致服务器的配置普遍过高,容易出现大量“只安装一个应用程序” 而未得到充分利用的 x86 服务器,同时缺少统一的集中化 IT 构建策略,无法对数据中心内的基础设施进行监控、管理、报告和远程访问。

2） 虚拟化后的迷茫期

为了解决集中的大规模 IT 基础设施资源利用率不足的问题,从计算虚拟化、存储虚拟化,到网络虚拟化、L4-L7 层服务虚拟化,以降低成本、提升 IT 运行灵活性、提升资源利用率为目标的各类虚拟化技术开始在政府数据中心中进行部署。

通过虚拟化技术,一方面可以提高硬件效率,另一方面也大幅提高服务器上线效率,服务器上线所需的时间从原来的以周或月为单位减少到现在的以小时或分钟为单位,大大改善了政府的业务应变能 力。

虚拟化技术的普及,改善了政府 IT 建设面临的成本支出和业务部署速度问题,同时也提高了设备利用率。但新技术的引入同时也带来了新问题和新需求。

在虚拟化前,每个业务系统具有独立的 IT 资源,虚拟化后,多个系统共享 IT 资源池,这样就会导致资源边界不明确,从而导致以下新问题:

随着虚拟化技术的大量应用,逻辑设备的数量增加,同时也带来了配置管理的工作压力,手动配置每一个虚拟设备并上线成为了管理员的噩梦,自动化需求应运而生;

应用管理员关注应用的部署,安全管理员关注安全策略的实施,而如何将应用和安全策略部署到 IT 基础架构,如何实现部署过程的便捷化,实现系统协同和资源整合,成为提升 IT 运行效率的关键。

当前的现实是,网络管理、存储管理、计算管理是割裂的三大系统，导致所有的应用和安全策略部署,不得不面临多系统的协同配合,以及大量的人工操作。如何实现应用在 IT 系统（服务器、存储、网络、终端系统） 的协同部署,智能化的自动化部署,实现更加高效,便捷的新 IT 架构,是摆在智慧园区大数据云中心面前最直接的问题.

13.1.6.2 云平台架构新思考

1） 政府 IT 基础架构演进

资源虚拟化、资源池化等技术的快速普及,使得 IT 基础架构资源的供给方式开始发生变化,以跨越异构、动态流转的资源池为基础提供给政府云中心可自治的服务方式逐渐成为新的趋势,IT 基础架构开始实现资源的按需分配、按量计费。

按需服务的新型服务模式导致资源规模化、集中化，让政务专有云的建设和运维统一集中到区政府云中心,各委办局单位更加关注于自己的业务和资源需求,从而提高了智慧园区大数据云平台建设的效率和弹性,让政府 IT 系统帮助和促进政府 IT 服务的转型，让政府信息中心成为一个价值部门,而不是永远停留在 IT 维护部门的角色。

在这种按需服务的建设思路下,各委办局数据中心都会逐渐统一在智慧园区大数据云中心部门下,实现政府 IT 建设的资源集中化、规模化,能够实现对各类异构软硬件基础资源的兼容,还能够实现资源的动态流转,支持异构资源和实现资源的动态流转,可以更好的利用资源,降低政府云计算基础设施建设成本。

各委办局单位无需自建基础系统,可以更加专注于自己的业务，委办局用户可按需获取基础设施资源,通过云中心的自服务门户,按需申请,按使用量付费和结算。

2） 自动化所面临的挑战

基础架构资源的整合,对计算、存储、网络的自动化和资源整合提出了新的挑战,并带动了一系列技术、架构、商业模式的变革。

传统模式下,服务器、网络和存储是基于物理设备连接的,因此，针对服务器、存储的访问控制、QoS 带宽、流量监控等策略基于物理端口进行部署,管理界面清晰,并且设备及其对应的策略是静态、

固定的。

在虚拟化的基础架构中,服务器、网络、存储等都采用了虚拟化技术,形成了资源池的概念和形态。所谓资源池（Resource Pool ），是一组可重用资源的集合,提供对外共享的资源服务,同时提供对于共享资源的管理机制,在集合（资源池） 中的资源可回收再分配,如下图所示。计算、网络、存储资源均实现可动态分配、回收、配置，在不牺牲效率、设备利用率和扩展性的前提下,降低了资本支出（CAPE） X 和运营支出（OPEX ）,提高了运行效率。

构建资源池的关键在于需要解决以下两个问题：

1 ） 虚拟资源的组成单位是什么,按照什么粒度来分配,是否可回收再分配?

2） 虚拟资源和物理资源的映射关系是什么,如何从物理资源上创建虚拟资源?

计算虚拟资源的最小粒度是以虚拟机为分配单元,存储虚拟资源的最小粒度是以存储空间或者虚拟卷为分配单元。而网络虚拟化的情况则最复杂,虚拟网络资源的最小粒度仅仅依靠虚拟网络设备是不够的,还需要解决虚拟网络路径的分配问题,这就意味着网络虚拟化需要同时处理设备虚拟化和路径虚拟化,将计算资源、存储资源、用户连接在一起的同时保障路径的隔离、独立和连通性,这是一个艰巨的任务。

挑战一：网络自动化,完成网络的虚拟化、实现自动化的网络路径连通性。只有网络能够充分感知到计算资源池、存储资源池和用户访问的动态变化,才能进行动态响应,为新创建的计算资源、存储资源提供即时的网络接入,同时保障网络的路径连通性和网络策略的一致性,让用户能够即时的访问到计算、存储资源。

为了解决网络虚拟化之后的自动化问题,网络控制器必不可少。

如果没有这个集中控制点,管理员就需要通过人工干预和手工配置虚拟网络老适应计算存储资源的变化,会大大降低云计算平台的灵活性、可扩展性。

作为网络资源池的唯一控制点,网络控制器需要实现网络虚拟化,通过网络分片实现网络的纵向隔离和虚拟化,通过网络节点虚拟化,自动为接入网络的计算资源、存储资源、用户提供接入策略、接入控制等服务,同时提供网络动态调整的能力,满足动态的网络容量规划要求。由于在基础架构层面实现网络、计算、存储、终端等资源相互联动的可行性很低,必须在虚拟控制层面打通,这就要求计算控制器、网络控制器、存储控制器之间能够进行有机的融合,形成一个统一的融合控制器。

挑战二：跨领域的资源管理和业务统一编排,实现计算、存储、网络资源的整合,形成一个有机的、可灵活调度和扩展的资源池,面向应用实现自动化的部署、监控、管理和运维。

而当前的现实是,网络管理、存储管理、计算管理是割裂的三大系统,应用管理员关注应用的部署,安全管理员关注安全策略的实施，所有的应用和安全策略部署,不得不面临多系统的协同配合,以及大量的人工操作。如何将应用和安全策略部署到 IT 基础架构,如何实现部署过程的便捷化,成为提升智慧园区大数据云平台运行效率的关键。

应用的部署不再仅仅限于单个领域资源的申请和使用,而是会跨越多个领域,使用计算、存储、网络、安全、LB、DNS 等各个领域的资源,通过引入跨领域的统一资源管理,能够更有效的利用资源,更快速的响应。

跨领域的资源管理解决的是资源的综合利用和资源统一管理问题,势必涉及到资源生命周期管理,包括资源申请、分配、回收、监控等,需要全新的交付模式和交付手段,自服务门户会逐渐成为虚拟资源管理的主要形式。

13.1.6.3 VCF 虚拟融合架构

当前由云端、网络、终端组成的云计算基础架构中,正经历着巨大的技术变革:BYOD 技术正将 IT 终端从传统的 PC 向智能化可移动终端演进； 传统数据中心向云转变,实现计算资源的弹性扩张,随需交付，应需而动。

而如何实现各种政府应用在云中的部署,如何实现各种终端基于安全策略的获取相应的应用服务,成为政务专有云需要关注的内容。

XXX VCF（Virtual Converged Framework ） 虚拟融合架构解决方案，则成为政务专有云的解决之道。VCF 架构自下向上分为三个层面（

1 ） 基础架构层

基础承载层包括端点、网络、计算、存储的基础设施,涉及政务专有云基础架构的全部设施,在网络部分不仅包含的传统网络,也增加了新网络技术如 OpenFlow、NFV、Overlay ； 终端实现了从传统 PC 到智能终端 (Apple IOS、安卓、Windows 8) 的管理； 数据中心部分包含服务器及其 Hypervisor 系统、存储、网络的集成和整体交付。

2） 融合控制层

融合控制层包括 VCFC、VCF-EIC、VCF-CAS （如图） ,分别实现对网络、终端、云计算的软件定义。

其中,VCFC 是 XXX SDN Controller ,提供了对传统经典网络、OpenFlow 网络、Overlay 网络、NFV 网络的支持和网络集中控制,更重要的是提供了基于 OF 的各种 SDNAPP,实现 SDN 的价值,如：软件定义的 L2、L3、QoS、TE 转发 APP、Overlay 转发 APP、服务 APP、SDNAPP 的大规模集群架构,以及基于 VCF Controller SDK 的第三方 APP。

VCF-CAS 实现了云计算的软件定义,实现 VM 的创建、迁移、克隆、快照等集中管理功能。

VCF-EIC 实现了终端的软件定义,实现对终端（不仅限于设备,还包括 iNode、iOS 等软件） 的安全认证、健康检查、MDM （Mobile DeviceManagemen）t 、MAM（Mobile Application Management ）的集中管理（MAM 可以根据策略实现应用在终端的推送和擦除） 。

3） 资源管理层

资源管理层实现面向端点/用户/应用的资源虚拟化,对计算、存储、网络等资源的统一自动化编排,以及资源的按需交付、应需而动。

基于 OpenStack,XXXCSM 云服务管理平台在实现网络业务编排的同时,可以支持计算、存储、数据库、安全、DNS 等各类资源申请、管理以及业务编排,并且提供完善的自服务门户,为政务专有云建设提供全套的运维、服务、管理、监控服务。

基于资源管理层,提供 Open API,支持基于 iMC VCF SDK 的第三方 APP,支持第三方软件对接,支持应用联动需求。

13.1.6.4 VCF 架构下的云平台

当前,政府逐步从“政府信息化” 走向“信息化政府” ,信息化政府的一切 IT 支撑活动都是基于各种应用业务系统开展的。政务专有云作为云中心的重点,其规划与设计不仅要满足业务需求,还会影响政府的整个 IT 应用架构,实现政府的 IT 服务转型,甚至推动政府行政架构的完善和管理变革。

xxx 认为,政府 IT 基础架构的发展和演进会依次走过标准化、虚拟化、自动化、业务驱动这几个阶段,最终完成向政府专有云模式的转变。

XXXVCF 通过软件定义架构,实现了应用在云计算系统（服务器、存储、网络、终端系统） 的智能化、自动化的协同部署,实现更加高效、便捷的智慧园区大数据云架构。

“设备、控制、平台、门户” 这不同的维度帮助政府完成一次转型,即向 IT 应用在终端、网络、云的端到端部署、以及向网站门户等不同层次的转型特别是控制层面,通过 XXXVCFController ,政务专有云建设可以明确面向应用的统一策略控制点,提供完整的网络策略控制,囊括终端接入控制、VM 接入控制等策略,还能提供 L4~L7 服务 的部署策略,这样应用部署、安全部署、VM 部署等都需要从 VCF Controller 获取 profile/ 策略,不仅实现面向网络、计算、存储部署策略的集中控制,还能为上层应用提供统一的策略入口和控制点。

在云计算时代,每天新增的数据量非常巨大,需要处理的数据也成倍增加,这就要求云平台具备更高的处理性能。传统的处理方式主要通过购买更高性能的设备来提升云平台性能,但是整个云平台的性能提升并不明显,主要原因在于云平台内部各组件各自为战,无法有效的协同工作。通过统一的控制器实现云计算基础架构的集中控制和调度,通过融合的管理平台实现面向应用的自动化运维,通过云网融合的云计算基础架构,能够实现云平台的协同工作,为各种云应用提供高效的云计算基础架构平台和技术指导。

13.1.6.5 云平台融合架构设计

委整体分为六大部分：

1） 、物理层

物理层包括运行云服务商平台所需的云数据中心机房运行环境，以及计算、存储、网络、安全等设备。云数据中心机房的部署按照分区设计,主要分为数据库区、业务应用区、存储区、系统管理区、网络出口区和安全防护区等区域。

2 ） 、资源抽象与控制层

资源抽象与控制层通过虚拟化技术,负责对底层硬件资源进行抽象,对底层硬件故障进行屏蔽,统一调度计算、存储、网络、安全资源池。其核心是虚拟化内核,该内核提供主机 CPU、内存、IO 的虚拟化 ,通过共享文件系统保证云主机的迁移、HA 集群和动态资源调度。同时通过分布式交换机实现多租户的虚拟化层的网络隔离。在存储资源池的构建上,采用分布式存储技术,实现对服务硬盘的虚拟化整合，并通过多副本（3-5 份） 技术保证存储数据的高可靠。

3 ） 、云服务层

云服务层提供 IaaS、PaaS 和 SaaS 三层云服务：

IaaS 服务：包括云主机、云存储（云数据盘、对象存储） 、云数据库服务、云防火墙、云负载均衡和云网络 （租户子网 /IP/ 域名等） 。IaaS 层服务向 PaaS 层提供开放 API 接口调用。

PaaS 服务：包括消息处理队列、通用中间件（请求代理、事物处理、地理信息） 、数据交换平台、开发测试平台,为上层政务应用提供标准统一的平台层服务,并提供 API 接口和 SDK 开发包,供 SaaS 层软件开发与部署调用。

SaaS 服务：包括本项目需要上线的 OA 协同办公平台、数字城管、综合治理、创新社会管理,以及政务网站群等,本层服务的提供由应用软件开发商完成。

上述云服务通过自助服务门户,向各委办局用户提供自助的线上全流程自动化交付。用户可以在自助服务门户上进行服务的申请,完成审批后相应的云资源将会交付给用户远程控制使用。

4 ） 、云安全防护

云安全防护为物理层、资源抽象与控制层、云服务层提供全方位的安全防护,包括防 DDoS 攻击、漏洞扫描、主机防御、网站防御、租户隔离、认证与审计、数据安全等模块。满足国家安全等级保护 3 级的部署要求。

5 ） 、运行监控与维护管理

此模块为云平台运维管理员提供设备管理、配置管理、镜像管理、备份管理、日志管理、监控与报表等,满足云平台的日常运营维护需求。

6 ） 、云服务管理

此模块主要面向智慧园区大数据云管理员,对云平台提供给委办局用户的云服务进行配置与管理,包括服务目录的发布,组织架构的定义,委办局用户管理、云业务流程定制设计以及资源的配额与计费策略定义等,此部分的功能实现根据市智慧园区大数据云要求进行定制。

13.1.7 xxx 网云平台方案

13.1.7.1 基础架构层

物理资源层应包括运行智慧园区大数据云所需的机房运行环境，以及计算、存储和网络等设备。

数据中心机房满足 GB 501 74-***8 《电子信息系统机房设计规范》中的 A 级要求,满足国际公认的 ANSI-TIA-942-***5 《数据中心通信基础设施标准》 里的 Tier 3 级以上主要指标。组网

设计采用“核心－接入” 两层扁平化设计 ， 根据模块化的分区的方式,主要分为业务应用区、云数据库区、管理和服务区、核心交换区和云安全访问控制区。

市政务专有云平台与电子政务专网的互联采用专用光纤,带宽不小于 2 条 10G,满足核心网络与业务系统互联的要求,两条 路 之 间通过网络虚拟化技术实现 路负载分担和互为备份。

13.1.7.1.1 设备选型

1） 计算设备选型

智慧园区大数据云数据中心随着服务器、存储、网络规模的成倍增加,硬件成本也水涨船高,同时管理众多的基础设施的维护成本也随着增加。传统 IT 基础设施建设往往采用机架式设备,一整套设施至少需要占用 1 个机柜的空间,各设备之间通过繁杂的线缆连接,维护较为困难。同时传统情况下服务器的利用率长期保持在 20%以下， 各设备间分开供电与散热,带来了大量的空间、电力、能耗等方面的浪费。

统一基础架构设备通过在一个刀箱中集成了服务器、存储、网络、虚拟化软件等设备,大大提高了服务器的利用率,减少了空间、电力、能耗等方面的消费。经测试统计得出,采用统一基础架构设备,可以提升至少 3 倍的服务器利用率,降低至少 75%的空间占用,减少至少 27%的电力消耗,降低初始购买和后期运维成本。为了降低数据中心的硬件成本和管理难度,对大量的 IT 硬件基础资源进行整合成了必然的趋势。

统一基础设施能够改善数据中心环境,令云服务商可以专注于创新,使科技成为改变业务的关键所在。共享服务池可在运行中随时调用,提高业务环境的灵活性,加速实现应用程序的价值。统一基础设施充分利用现有的技术投资,消除数据中心的技术设备冗积问题,化繁为简。通过统一的管理,所有资产都成为资源池的一部分,能够分割、组合、变化,动态适应任何业务、负载或应用的需求。这些资源 的使用也经过优化,帮助云中心提高利用率,降低使用能耗和成本。

（2） 存储设备选型

存储设备作为云计算 IAAS 建设模型里三大基础硬件之一,整体存储系统需要面向所有业务模块并适应服务器虚拟技术的存储使用，服务器虚拟环境中对存储 I/O 决定着虚拟化应用性能和业务处理能力（I/O 瓶颈） 。

政务专有云的数据文件存储需求主要分为两种,一种是为资源池中的虚拟机文件系统和虚拟机本地数据提供共享存储空间,便于虚拟机的快速迁移和高可用 HA 和本地数据快速存取,另一种是为数据库的结构化数据提供独立存储空间,实现数据库高速读写和数据安全。

虚拟化存储解决方案

在智慧园区大数据云数据库应用环境中,由于业务系统增长迅速,传统存储设备的物理性能和容量配置已经不能满足云计算发展要求,往往需要新购一台数据库存储设备接管现有存储设备的性能和容量,并希望能为未来的发展提供充足的扩展空间,为未来的云中心容灾建设提供安全、高效、经

济的硬件平台支持。

本次政务专有云部署的数据库专用存储设备需能够解决传统存储设备在实际维护和使用的过程中遇到的如下困难：

存储扩容步骤复杂,费时费力,整个扩容过程很难保证数据完整性

存储扩容后容易导致应用系统的 IO 性能下降

存储配置调整复杂,特别是对于 RAID 组或 LUN 的配置进行调整

无法对存储的热点数据进行自动监控和优化

当磁盘出现损坏时,存储设备的全局热备盘重建时间长,重建时影响系统性能

那么采用 3PAR 虚拟化存储能够很好的解决以上数据库传统存储遇到的头疼问题,3PAR 的技术先进性为政务专有云的应用数据库提供优异的性能和出色的功能支撑。

存储服务器采用全分布式架构,通过一个高带宽、低延迟特性的背板,将经济高效、模块化、可升级的组件统一成一个具有高可用性的、可自动均衡负载的集群。其独特的架构使得单台性能大大超越传统的存储。

独特的双分类处理单元

内嵌 ASIC 技术使存储设备可以支持混合工作负载,从而减轻性能负担,降低了传统阵列的成本。使用独特的双分类处理单元,交易 数据处理和吞吐量密集型工作负载再也不必争用相同的存储资源。它是通过使用 ASIC 和相关的数据缓存,在每个控制器节点内并行迁移数据； 同时,使用 Intel CPU 和相关的控制缓存来处理元数据而实现的。

全新的磁盘划分方式

存储设备在后端磁盘管理的方式与其他传统存储系统截然不同，传统存储设备只能按照单颗物理磁盘进行管理,而 3PAR 会将单颗物理磁盘划分为以 256MB 为基础单元的存储小块。

根据磁盘的不同类型,可以将存储小块统一放入不同的资源池进行统一管理,所有的逻辑卷是由存储资源池中的数个存储小块组成。

通过这种方式可以使逻辑卷的存储空间管理更灵活,扩容更方便简单,此外还能使逻辑卷的存储空间均匀分布在存储后端的各块磁盘上,极大的提升性能,提高整个存储的性能利用率。

通过 3PAR 特有的磁盘管理方式,对逻辑卷的扩容操作变得异常方便.

高性能存储系统

存储设备的高性能主要源自以下几个方面：

1） 全网状的控制器设计,多控制器可以同时对单个逻辑卷进行读写操作,提高了存储系统的并发读写能力

2） 双分类处理器设计,将存储控制流和传输流的分类,提高了 IO 的处理和响应能力

3） 存储小块的管理方式,使单个逻辑卷的存储空间均匀的分布在后端所有磁盘驱动器上,充分的发挥了存储后端的性能

4） 自动分层存储和热点数据迁移,通过智能化监控和调优提升了存储的性能

存储的高可用性

存储设备的可扩展架构下,多节点为客户提供了更高的冗余度,一个甚至多个节点的故障不会对系统的连续性甚至是性能造成影响（采用持续缓存技术情况下） 。四个节点的部署情况下，当一个存储节点意外停机时,不会进行缓存停用,而将缓存中的数据重新在另外三个节点上进行重新部署,以保证读写性能不受影响。

同时 3PAR 独特的存储架构可以提供用户不同的存储高可用隔离级别,通过设置不同隔离级别,可以允许同一个磁盘组或者同一个磁盘柜的磁盘损失的情况下,系统数据不丢失，此外,由于采用了256MB 的存储小块作为基本能单位,所以当物理磁盘发生故障时,热备盘的重建是以存储小块为基础进行的,所以重建工作可以分布在不同的物理磁盘上,进行多对多的重建,大大缩短了恢复的时间。

虚拟资源调配

虚拟资源调配技术是一项绿色存储技术,可为智慧园区大数据云大幅度节省不必要的存储开销,简化系统管理工作。

它可以使得用户先为应用提供虚拟容量,一次给前端应用配置最大虚拟空间,但真正物理容量购买是根据实际应用写入的数据而定。

3PAR 的虚拟资源调配技术与其他同类技术相比,做到真正的不需预留空间、按需分配,并且在存储池中根据需要,以微增量配置容量,无需大块数据单元的预分配,从而帮助用户高效的配置存储空间,杜绝浪费。

此外通过虚拟资源调配技术,可以为应用系统分配最大的虚拟容量,能有效的减少了应用系统扩容的次数。

3PAR 虚拟资源调配技术能够与 Oracle 数据库 ASM 特性很好的配合使用。通过为 Oracle 数据库提供可以按照实际写入自由分配空间的虚拟逻辑卷,充分结合 Oracle ASM 的特性,保证了数据库存储空间管理的简便和一致,通过 Oracle 公司的实际测试,P8000 存储设备的虚拟资源调配功能可以提供与普通存储卷基本相同的性能：

（3） ） 核心交换机选型

在政务专有云建设中,由于网络位置的特殊性和关键性,对核心设备都有着一致的更高的要求：更高的可靠性、更大的处理能力、更高的扩展性、更精细化的业务调度能力。面对上述要求,选择什么样的核心设备,或者说选择什么架构的核心设备成为关键。

业界当前的核心交换机主要有两种架构：采用单级单平面交换网（基于单个 crossbar 或者几个 crossbar 简单累加） 的第五代交换机，和采用多级多平面交换架构的第六代交换机,下面简单比较两者的差别。

交换架构的扩展性

单级单平面的交换架构,交换容量依赖单颗 crossbar(交换网片)的交换容量,而单颗 crossbar 网片的交换容量到达一定程度后,已经无法再发展下去（否则芯片内部过于复杂） ,目前业界单颗 crossbar 的交换容量已经发展到了极限（单颗几百 Gbps）,为了实现更大的交换容量,第五代交换机只能将少数几颗 crossbar 交换网片简单的叠加起来,从而最多提供 1 .xTbps 的交换容量。

交换架构的可靠性

对于单级交换架构的设备,从实现经济性的角度,都是将交换引擎集成于主控板上,造成转发平面和控制平面在物理上并没有分离,从而控制平面的故障会影响转发平面的工作,设备可靠性受到影响。

另外对于单级交换设备往往设计为两块主控板上的交换网负荷分担才能满足系统交换容量的要求 （再一次体现了单颗交换网片容量的限制） ,此时如果一块主控板故障（不论是转发还是控制导致的故障） ，系统交换容量只能减半。可以看出,由于转发平面和控制平面没有物理分离,导致转发平面必须额外承受控制平面故障带来的影响。

而多级多平面交换架构的设备,交换网片承载于独立的交换网板,使得转发平面和控制平面物理上彻底分离,这样如果主控板发生了故障,只要由另一块主控板进行控制平面的 1 +1 冗余备份,对交换网没有任何影响,使得转发平面完全独立于单个控制平面的故障,可靠性大大增强。并且由于多级多平面交换架构的核心交换机,交换网之间多是 N+1 的冗余,一块交换网片故障对系统的交换容量没有任何影响,即使发生多块交换网片的故障,系统的交换容量也只是平滑的逐级下降,将对数据转发的影响降到最低。

业务调度的无阻塞性

单级交换架构的设备,为实现更大交换容量,采用几颗交换网片简单叠加时,从源端口到目的接口板的数据往往采用固定路径转发方式， 不能充分利用系统交换带宽,存在特定情况下的阻塞现象。

采用 CLOS 架构的多级多平面交换架构的设备,全部路径通过严格的数学推算,可以实现真正的无阻塞交换。

从上面的技术分析可以看出,多级多平面交换架构在构建大容量、高可靠、高扩展性下一代核心交换机上具有单级交换架构无可比拟的优势。从智慧园区大数据云网络建设的角度来说,一张云网络的建设考虑的不仅仅是当前的应用,而是今后几年的应用。而随着业务的发展,对网络的带宽要求往往是超预期增长的,考虑核心设备的特殊性和关键性,核心设备的选择往往决定了今后网络的扩展性。在业界主流厂商已经纷纷推出基于多级多平面交换架构第六代核心交换机的今天,对于建设一个技术先进的政务专有云来说,云平台网络核心建议采用基于多级交换架构 CLOS 的核心交换机无疑是更好的选择。

13.1.7.1.2 专享业务区

主要用于部署承载业务应用的 2 路机架式服务器,通过提供大内存高性能机架服务器,作为计算单元。同时配置 SAN 存储做成存储集群,为虚拟机的系统镜像和数据提供集中存储资源。

单台物理服务器分别连接四个不同的网络：

1 、业务网络：服务器 1 0G 网卡通过上联 TOR 万兆交换机,提供业务数据访问网络；

2、管理网络：选用 6 台机架服务器网卡通过上联万兆机架交换机,通过系统管理区相应管理软件实现虚拟化平台管理、网络管理、XXX CSM 管理等；

3、存储网络：通过服务器网卡上联万兆存储 TOR 交换机,实现不同区域不同物理主机之间存储

网络的互通；

4、服务器带外管理网络：通过服务器带外管理 iLO 口上联万兆 TOR 管理交换机,形成跨交换机带外管理网络集群,方便运维人员以服务器集群为单位对硬件进行统一管理配置。

13.1.7.1.3 管理和服务区

部署云管理平台、网络管理平台、虚拟化管理平台等管理服务器，硬件采用大内存高性能 2 路机架服务器。通过对云管理平台、网络管理平台、虚拟化管理平台等软件的部署,实现对底层资源的合理管控，保障业务运行的可靠性、可用性,合理的分配资源,通过自动化的运维管理,提升客户 IT 人员的运维管理效率.

从业务管理可靠性来分析,系统管理区各管理平台部署分为两大类,硬件支撑系统和虚拟支撑系统。

硬件支撑系统主要是考虑到业务管理平台的重要性和可靠性,故直接采用物理服务器作为支撑平台,包括：

1 、XXX CVM 双机集群：通过 CVM 主机实现对虚机的管理运维，采用双机热备的形式,保证 CVM 管理平台的可靠性

2、XXX CSM 双机集群:通过 CSM 主机实现对大云平台的管理运维,采用双机热备的形式,保证 CSM 管理平台的可靠性虚机支撑系统是指在虚拟化环境下,直接将管理平台部署在虚机上,建立统一的云服务管理集群,通过虚拟化软件来保证各管理平台的可靠性,在 CVM 集群内主要运行以下几个系统：

数据库管理：主要内容包括数据库的建立、调整、重构、安全控制、完整性控制和对用户提供技术支持。

XXX 运维管理平台：实现网络拓扑、故障、性能、配置、安全等管理功能。

OpenStack 计算管理节点：对下层虚拟化计算资源进行管理调度。

对象存储管理：静态数据的存储、检索、预览,数据的持久性和可扩展性管理。

13.1.7.1.4 云数据库区

部署承载数据库服务的物理服务器,对于部分高性能数据库可直接部署在物理机架服务器上,通过配置 4 路高性能机架服务器,来满足客户对于数据库系统的承载需求。对于性能要求不高的数据库服务,以虚拟机方式部署交付。数据库服务区通过部署高性能的 FC 存储,来满足客户关键业务的数据存储以及对数据。核心交换区

通过物理网络设备 N:1 虚拟化技术,简化生成树协议的部署,实现云数据中心内的大二层网络互通,为云主机的自动化迁移与调度提供环境支撑,核心交换区的主要功能是完成各服务器功能分区、广域网、互联网之间数据流量的高速交换,是广域/局域纵向流量与服务功能分区间横向流量的交汇点。核心交换机必须采用专业的 CLOS 架构数据中心级交换机,具备高速转发的能力,同时还需要有

很强的扩展能力，以便应对未来业务的快速增长。两台核心交换机部署双机虚拟化功能,服务器接入交换机通过聚合 路上联到核心交换机,服务器接入交换机可以实现双上行 路双活使用,提高 路的使用效率； 要求服务器接入交换部署相同的虚拟化技术。虚拟化系统可以实现设备级、路级故障毫秒级恢复。

为了保证核心平台的可靠性,部署两台数据中心级核心交换机，两台设备通过物理网络设备 N:1 虚拟化技术实现双机虚拟化功能,保证设备级和 路级的毫秒级故障恢复。同时双机虚拟化简化生成树协议的部署,实现云数据中心内的扁平化二层网络互通,为云主机的自动化迁移与调度提供环境支撑。同时在核心层旁挂服务器负载均衡设备 LB,提供服务器业务系统的负载均衡,提高访问效率。

核心区使用 路聚合技术合并多个 40GE 端口,提供两交换机之间的连通性。核心区交换机连接到所有其他区的边缘设备,既可以是一对 HA 方式的交换机,也可以是一对 HA 方式的防火墙。有两类连接到核心,一类是来自交换机 （比如业务系统服务器区） 的连接，另一类是用防火墙连接（互联网接入区） 。每个区边缘交换机都上行连接到 Core-SW1 和 Core-SW2。每个区交换机将使用单独的 VLAN,VLAN 跨越两个交换机,上行连接到核心。成对且以高可用性方式部署的防火墙将有一个 VLAN,这个 VLAN 跨越两个核心交换机上行连接,并每 个都连接到一个核心。每个上行连接 VLAN 都在两个交换机中配置。

13.1.7.1.5 安全访问区

此区域是逻辑区域,用于部署与电子政务专网、多云中心之间进行数据交互的安全隔离设备,确保数据访问安全,包括设置网络隔离、防火墙、IPS、端口安全检测、漏洞扫描和日志安全审计等。保证物理网络安全性的同时,通过虚拟化技术,实现在虚拟化环境下数据访问的安全控制,此区域实现的功能：

1 、访问控制：利用防火墙实现云数据中心的整体安全防护； 同时为每个申请安全服务的租户提供独立的 vFW 服务,实现租户业务的隔离需求。

2、入侵防御：在出口防火墙后端部署高性能 IPS 模块,实现 IPS 在线部署。通过 IPS 设备,可为数据中心内部提供了更坚固的安全保护机制。通过 IPS 的深度检测功能可以有效保护内部服务器避免受到病毒、蠕虫、程序漏洞等来自应用层的安全威胁。

3、堡垒机设备：部署堡垒机设备提供对物理设备访问时的安全跳转平台，一方面可以防止非法用户直接登录物理设备带来的安全隐患,另一方面可以有效授权并记录合法用户的操作。

4、路负载均衡功能：实现对智慧园区大数据云数据中心 路负载均衡的功能,以充分利用多出口路。

5、SSLVPN 网关设备：VPN 设备自带 SSLVPN 功能,可以满足用户通过互联网安全访问智慧园区大数据云内部数据中心业务的需求,实现远程移动办公；

6、对于数据中心服务器内部虚拟机之间的安全控制防护可以采用虚拟机承载的虚拟机形态防火墙设备进行安全防控。

13.1.7.2 资源融合控制层

传统的 IT 基础架构建设模式已经不能适应政府云计算建设要求,需要有一种新的 IT 建设模式来改变政府 IT 头重脚轻的这种不平衡架构。为了摆脱上述困境,必须要从全局出发,把云端、网络和终端综合起来进行考虑。对于云端,采用先进的虚拟化技术和集中控制的方式,提高服务器利用率,控制服务器数量,提高业务响应速度，降低成本； 对于网络来说,通过网络控制器的方式简化网络架构,网络控制器与云端控制器的联动,实现基于应用的网络自动化部署和面向应用的网络管理,通过开放控制器软件接口的方式实现网络软件定义,从而实现新技术的快速部署； 对于终端,必须通过控制器的方式实现传统终端和智能终端的统一控制、无线、有线和 VPN 的统一控制、终端安全和网络接入的融合控制、移动办公网络融合控制。同时,在控制器层面通过软件接口把云网端协同联动起来,当业务发生改变时,云计算平台能够及时感知并进行自动化的适配。减少人工干预，从而提高整个云计算平台的效率。

VCF 通过一种架构来承载所有业务,其基本思想是借鉴了 SDN 控制与转发分离的设计理念,通过统一的控制器来集中管理基础架构，使上层应用与底层架构解耦,解决当前云计算平台基础架构所面临的问题。

13.1.7.2.1 融合控制体系

融合控制体系在 VCF 架构中处于云管理平台与基础硬件系统中间,通过它来屏蔽硬件架构的差异,对上层应用系统提供标准的接口,使 IT 系统标准化,它包括 VCFC（即 VCF 控制器） 、VCF-EIC、VCF-CAS ,分别实现对网络、终端、云端的集中管控。

VCF 融合控制体系,对下统一控制软硬件网络设备、应用交付设备、计算设备、存储设备以及终端设备,对上提供各种软硬件单元抽象和策略定义,实现终端、网络、计算、存储等要素的统一呈现与配置； 基于应用的服务功能 定义,为资源平台提供统一的北向调度接口,为上层的业务系统提供一个虚拟化层,从而使用户从复杂的硬件系统中摆脱出来,把精力投入到应用创新中去,发挥更大的价值。通过融合控制体系,IT 基础设施建设可以明确面向应用的统一策略控制点,提供完整的基于应用的策略控制,囊括终端接入控制、VM 接入控制等策略,还能提供 L4~L7 服务 的部署策略,这样应用部署、安全部署、VM 部署等都需要从 VCF 控制器获取 profile/ 策略,不仅实现面向网络、计算、存储部署策略的集中控制,还能为上层应用提供统一的策略入口和控制点。

13.1.7.2.2 网络控制器

云计算、大数据等新 IT 应用已经成为政府信息化发展的趋势,为适应新应用的部署,各种服务器虚拟化、存储虚拟化技术快速发展，但是整个智慧园区大数据云平台的效率并没有显著的提升,反而使智慧园区大数据云平台的运维变得更加复杂,究其原因在于网络技术的发展无法满足服务器

虚拟化及存储虚拟化技术发展的要求。通过类 SDN 的网络虚拟化解决方案,兼容标准 OpenFlow 网络的同时融合传统网络,该方案关键在于通过集中控制的方案简化网络架构、简化运维、实现对网络对应用的感知,最终实现面向应用的网络自动化运维。

VCFC 集成了 XXX Comwar 网 e 络操作系统和开源的 OpenDaylightSDN 控制器,拥有丰富的适用于数据中心、园区网、运营商、WLA 无 N[1]线网等多种网络环境的应用程序,同时具备 OpenDaylight 的开放架构,支持 OpenDaylight 标准开放接口,第三方基于 OpenDaylight 接口开发的 SDN 应用程序,可无缝的运行于 VCFC。

VCFC 北向 API 兼容 Comware 网络 API,Comware 应用程序可运行于 VCF 控制器。这些 Comware 网络应用,提升了 SDN 网络的适用范围,为 SDN 创新网络和传统网络结合提供了可能。

VCFC 南向接口,既支持 OpenFlow、BGP-I2RS、PCEP 等 SDN 新型控制协议,也支持 SNM、P NETCON、FOVS-DB 等传统网络管理协议。进一步,VCFC 南向接口集成了 ComwareOpenSDK,利用网络设备的开放 API 能力,在 VCFC 远程集中控制远程网络设备。

VCF 架构超越了单 的 OpenFlow 集中式控制理念,通过融合传统网络控制技术和 SDN 集中控制技术,实现了网络技术的平滑演进。如图 3 所示,VCFC 可看作是 IRF 技术演进和 OpenFlow 集中控制技术的融合。VCFC 即可控制传统网络设备,也可控制 NFV 虚拟服务单元和 OpenFlow 交换机,提供了一致性的 SDN 部署体验。

13.1.7.2.3 虚拟化管理平台

XXX CVM 虚拟化管理系统是 XXX CAS 核心组件之一,主要实现对政务专有云内的计算和存储等资源池的管理和控制,对上层应用提供自动化服务。

CVM 平台可以集中管理数千台物理服务器和数万台云主机,通过一个统一的管理平台来对所有相关任务进行集中管理,管理员仅需要键盘和鼠标便可实现云主机的部署、配置和远程访问等操作虚拟化管理系统可以实现以下功能：基于集群的集中管理、共享存储管理能力、虚拟交换机管理、资源使用状况监控。

① 基于集群的集中管理;

XXX CAS CVM 虚拟化管理系统将服务器主机和云主机都组织到集群中,单个集群支持 5000 台以上的物理机,1 PB 以上的分布式共享文件系统存储,另外单个集群支持的并行任务调度数量不低于十万级。提供了清晰的分层结构视图,直观地展示了数据中心、主机池、集群、主机和云主机之间的关系,大大简化了资源管理的工作量。

基于集群进行集中管理的好处在于：

利用集中化管理功能,管理员能够通过统一的界面对整个 IT 环境进行组织、部署、监控和配置,从而降低管理成本。

由多台独立服务器主机聚合形成的一个具有共享资源池的集群不仅降低了管理的复杂度,而且具有内在的高可用性,通过监控集群下所有的主机,一旦某台主机发生故障,XXX CAS CV 虚 M 拟化管

理系统就会立即响应并在集群内另一台主机上重启受影响的云主机,另外支持集群的在线扩容,从而为用户提供一个经济有效的高可用性解决方案。

② 共享存储管理

XXX CAS CVM 虚拟化管理系统中的虚拟机文件系统是一种优化后的高性能集群文件系统,允许多个计算节点同时访问同一虚拟机存储。由于虚拟架构系统中的虚拟机实际上是被封装成了一个档案文件和若干相关环境配置文件,通过将这些文件放在 SAN 存储阵列上的文件系统中,可以让不同服务器上的虚拟机都可以访问到该文件,从而消除了单点故障。

③ 虚拟交换机管理

虚拟交换机是用软件实现的 IP 报文转发与控制模块。在物理环境中,物理服务器通过物理交换机连接到网络,在云平台中,云主机通过虚拟交换机连接到网络。为了让维护人员直观易懂,在 XXX 的虚拟化管理系统里会对虚拟交换机有一个直观易懂的管理界面

XXX CAS 虚拟交换机在设计时将整个虚拟交换机以物理交换机的面板呈现,并通过绿色的,闪烁的端口表示云主机连接虚拟交换机的 vNIC，每一个闪烁的绿色端口都表示一个活动的虚拟端口,可以显示端口名称、连接端口的云主机名称、云主机 vNIC 对应的 MAC 地址等。

④ 性能状况监测,包括如下监测参数；

物理服务器性能状态监测：提供物理服务器 CPU 和内存等计算资源的图形化报表及运行于其上的云主机利用率 TOP5 报表,为管理员实施合理的资源规划提供详尽的数据资料。

云主机性能状态监测：提供云主机 CPU、内存、磁盘 I/O 、网络 I/O 等关键资源进行全面的性能监测。

虚拟交换机状态监测：提供虚拟交换机上各个虚端口的流量统计与模拟面板图形化显示。

虚拟网卡性能状态监测：提供进出云主机虚端口流量的图形化实时显示。

13.1.7.2.4 计算资源池构建

服务器是云计算平台的核心,其承担着云计算平台的“计算” 功能。对于云计算平台上的服务器,通常都是将相同或者相似类型的服务器组合在一起,作为资源分配的母体,即所谓的服务器资源池。在这个服务器资源池上,再通过安装虚拟化软件,使得其计算资源能以一种云主机的方式被不同的应用和不同用户使用。在 x86 系列的服务器上,其主要是以 XXXloud 云主机的形式存在。后续的方案描述中，都以云主机进行描述,如下为 XXX 虚拟化软件的构成。

CVK：Cloud Virtualization Kernel ,虚拟化内核平台运行在基础设施层和上层操作系统之间的“元” 操作系统,用于协调上层操作系统对底层硬件资源的访问,减轻软件对硬件设备以及驱动的依赖性,同时对虚拟化运行环境中的硬件兼容性、高可靠性、高可用性、可扩展性、性能优化等问题进行加固处理。

CVM：Cloud Virtualization Manager ,虚拟化管理系统主要实现对数据中心内的计算、网络和存储等硬件资源的软件虚拟化,形成虚拟资源池,对上层应用提供自动化服务。其业务范围包括：

虚拟计算、虚拟网络、虚拟存储、高可靠性（HA）、动态资源调度（DRS）、云主机容灾与备份、云主机模板管理、集群文件系统、虚拟交换机策略等。

采用 XXX 的 CAS 虚拟化平台对多台服务器虚拟化后,连接到共享存储,构建成计算资源池,通过网络按需为用户提供计算资源服务。

同一个资源池内的云主机可在资源池内的物理服务器上动态漂移,实现资源的动态调配。

计算资源池的构建可以采用以下四个步骤完成：计算资源池分类设计、主机池设计、集群设计、云主机设计四个部分完成。

计算资源池分类设计

在搭建服务器资源池之前,首先应该确定资源池的数量和种类，并对服务器进行归类。归类的标准通常是根据服务器的 CPU 类型、型号、配置、物理位置和用途来决定。对云计算平台而言,属于同一个资源池的服务器,通常就会将其视为一组可互相替代的资源。所以，一般都是将相同处理器、相近型号系列并且配置与物理位置接近的服务器——比如相近型号、物理距离不远的机架式服务器。在做资源池规划的时候,也需要考虑其规模和功用。如果单个资源池的规模越大，可以给云计算平台提供更大的灵活性和容错性：更多的应用可以部署在上面,并且单个物理服务器的宕机对整个资源池的影响会更小些。

但是同时,太大的规模也会给出口网络吞吐带来更大的压力,各个不同应用之间的干扰也会更大。

初期的资源池规划应该涵盖所有可能被纳管到云计算平台的所有服务器资源,包括那些为搭建云计算平台新购置的服务器、政府内部那些目前闲置着的服务器以及那些现有的并正在运行着业务应用的服务器。在云计算平台搭建的初期,那些目前正在为业务系统服务的服务器并不会直接被纳入云计算平台的管辖。但是随着云计算平台的上线和业务系统的逐渐迁移,这些服务器也将逐渐地被并入云计算平台的资源池中。

针对政务专有云的需要,我们按照用途将云计算资源池划分为云主机&云存储区资源池、管理和服务区资源池,以便云计算平台项目实施过程以及平台上线以后运维过程中使用。

在云计算平台搭建完毕以后,服务器资源池可以如下图所示：

XXX CVM 虚拟化管理平台体系将云计算资源池的物理服务器资源以树形结构进行组织管理.

1 ） 主机池设计

完成在云计算软件体系架构中,主机池是一系列主机和集群的集合体,主机可纳入群集中,也可单独存在。没有加入集群的主机全部在主机池中进行管理。

2) 集群设计

集群目的是使用户可以像管理单个实体一样轻松地管理多个主机和云主机,从而降低管理的复杂度,同时,通过定时对集群内的主机和云主机状态进行监测,如果一台服务器主机出现故障,运行于这台主机上的所有云主机都可以在集群中的其它主机上重新启动,保证了数据中心业务的连续性。

3) 云主机设计

每台云主机都是一个完整的系统,它具有 CPU、内存、网络设备、存储设备和 BIOS,因此操作系统和应用程序在云主机中的运行方式与它们在物理服务器上的运行方式没有任何区别。与物理服务

器相比,云主机具有如下优势：

在标准的 x86 物理服务器上运行。

可访问物理服务器的所有资源（如 CPU、内存、磁盘、网络设备和外围设备） ,任何应用程序都可以在云主机中运行。

默认情况,云主机之间完全隔离,从而实现安全的数据处理、网络连接和数据存储。

可与其它云主机共存于同一台物理服务器,从而达到充分利用硬件资源的目的。

云主机镜像文件与应用程序都可以封装于文件之中,通过简单的文件复制便可实现云主机的部署、备份以及还原。

具有可移动的灵巧特点,可以便捷地将整个云主机系统 （包括虚拟硬件、操作系统和配置好的应用程序） 在不同的物理服务器之间进行迁移,甚至还可以在云主机正在运行的情况下进行迁移。

可将分布式资源管理与高可用性结合到一起,从而为应用程序提供比静态物理基础架构更高的服务优先级别。

可作为即插即用的虚拟工具 （包含整套虚拟硬件、操作系统和配置好的应用程序） 进行构建和分发,从而实现快速部署。

在计算资源池中,一般物理服务器与云主机的整合比平均不超过 1 :8 、单台物理服务器上所有云主机 vCPU 之和不超过物理机总内核的 1.5 倍、单台物理服务器上所有云主机内存之和不超过物理内存。

在构建完计算资源池后,软件本身还需要保证整个计算资源池及应用的易用性和可靠性,XXX CAS 虚拟化软件通过以下技术实现可用性和可靠性的要求：

1 ） 云主机模板设计

云主机模板包括云主机的 vCPU、内存等参数,主机根据主要应用系统负载量的不同提供不同的规格。

在采用云计算来向用户交付服务时,用户通过云门户自助申请的 IT 服务资源就是业务应用模板,因此需要提前设计好相应的 IT 服务模板向云门户发布,当用户申请该服务时,云平台根据模板进行资源编排,快速生成云主机相关资源交付给用户使用。

2) 高可用性设计

高可用性包括两个方面：

1． 云主机之间的隔离：每个云主机之间可以做到隔离保护,其中一个云主机发生故障不会影响同一个物理机上的其他云主机；

2. 物理机发生故障不会影响应用：故障物理机上运行的云主机可被自动迁移接管,即云主机可以在同一集群内的多台服务器之间进行迁移,从而实现多台物理服务器的之间的相互热备,实现当其中一个物理服务器发生故障时,自动将其上面的云主机切换到其他的服务器,应用在物理机宕机情况下保证零停机。

XXX CAS 虚拟化平台 HA 功能会监控该集群下所有的主机和物理主机内运行的虚拟主机。当物理主机发生故障,出现宕机时,HA 功能组件会立即响应并在集群内另一台主机上重启该物理主机内

运行的云主机。当某一发生故障时,HA 功能也会自动的将该云主机重新启动来恢复中断的业务。

3) 动态资源调度

动态资源调度功能可以持续不断地监控计算资源池的各物理主机的利用率,并能够根据用户业务的实际需要,智能地在计算资源池各物理主机间给虚拟机分配所需的计算资源。通过自动的动态分配和平衡计算资源,动态资源调整特性能够：整合服务器,降低 IT 成本，增强灵活性； 减少停机时间,保持业务的持续性和稳定性； 减少需要运行服务器的数量,提高能源的利用率。

动态资源调度功能组件可以自动并持续地平衡计算资源池中的容量,可以动态的将云主机迁移到有更多可用计算资源的主机上,以满足虚拟机对计算资源的需求。即便大量运行 SQLServer 的虚拟机，只要开启了动态资源调整功能,就不必再对 CPU 和内存的瓶颈进行一一监测。全自动化的资源分配和负载平衡功能,也可以显著地提升数据中心内计算资源的利用效率,降低数据中心的成本与运营费用。

动态资源调整功能通过心跳机制,定时监测集群内主机的 CPU 利用率,并根据用户自定义的规则来判断是否需要为该主机在集群内寻找有更多可用资源的主机,以将该主机上的云主机迁移到另外一台具有更多合适资源的服务器上。

4) 动态资源扩展 DRX 特性

计算虚拟化简化了部署业务服务器的流程和具体工作,极大的缩短了新业务服务器的部署周期,使得通过快速增减业务服务器来应对业务访问量的突发性变化成为可能。因此,部署了云业务环境的用户开始考虑采用动态部署方式来应对业务访问的突发性需求。但采用动态资源部署方式的一个不能忽略的前提是：IT 管理人员能够对业务访问量的突发性变化具备很强的敏感性,并且能够迅速采取应对措施。但当前的 IT 基础架构中,业务负载监控平台、虚拟服务器管理平台和业务分发的系统之间往往是割裂的,没有整合形成统一方案。

IT 管理人员在感知到业务访问变化时,只能通过手工进行虚拟服务器的增减和在业务分发系统的相应配置。这无疑缺乏灵活性且效率低下。

针对这些需求,XXX CAS 虚拟化平台可以实现面向应用的云动态资源扩展解决方案 DRX,如下图所示。XXX 虚拟化管理系统能够监测到业务所在云主机性能不足,并将云主机进行快速复制,配合负载均衡设备对外提供服务,当访问高峰过后,虚拟化管理系统能够动态的收缩,删除过剩的云主机,从而实现计算资源随需而动。

服务器虚拟化技术的出现使得计算服务提供不再以主机为基础，而是以云主机为单位来提供,同时为了满足同一物理服务器内云主机之间的数据交换需求,服务器内部引入了网络功能部件虚拟交换机 vSwitch （Virtual Switch ）,如下图所示,虚拟交换机提供了云主机之间、云主机与外部网络之间的通讯能力。

vSwitch 的引入,给云平台基础网络的运行带来了多租户的隔离问题：

由于云主机及服务器数量的增多,网络技术方案需要保证多个租户使用的资源能够有效的隔离,xxx 以 Overlay 的虚拟化方式用来支撑云与虚拟化的建设要求,并实现更大规模的多租户能力。

Overlay 的本质是 L2 Over IP 的隧道技术,xxx 相应的技术方案称为 Vxlan ,目前在服务器的

vSwitch 、物理网络上技术框架已经就绪。Vxlan 网络架构有多种实现,就 大二层的实现,可分为主机实现方式和网络实现方式； 而在最终实现 Vxlan 与网络外部数据连通的连接方式上,则有多种实现模式,并且对于关键网络部件将有不同的技术要求,包括基于主机的 Vxlan 虚拟化网络、基于物理网络的 Vxlan 虚拟化两种大的实现方式。在已经进行虚拟化的环境下我们将采用基于主机的 Vxlan 虚拟化网络方案,Vxlan 运行在 UDP 上,物理网络只要支持 IP 转发,则所有 IP 可达的主机即可构建一个大范围二层网络。这种 vSwitch 的实现,屏蔽了物理网络的模型与拓扑差异,将物理网络的技术实现与计算虚拟化的关键要求分离开来,几乎可以支持以太网在任意网络上的透传,使得云的计算资源调度范围空前扩大。

另外由于 Vxlan 把 1 2 bit 的 VLAN tag 扩展成了 24 bit ,这样能实现远远高于传统 VLAN 4096 的数量,解决了 VLAN 数量不足的问题,满足更多的租户隔离需要。

为了使得 Vxlan Overlay 网络更加简化运行管理,便于云的服务提供,XXX 使用集中控制的模型,将分散在多个物理服务器上的 vSwitch 构成一个大型的、虚拟化的分布式 Overlay vSwitch ,只要在分布式 vSwitch 范围内,虚拟机在不同物理服务器上的迁移,便被视为在一个虚拟的设备上迁移,如此大大降低了云中资源的调度难度和复杂度。

对于计算资源丰富的数据中心,Overlay 网络使得虚拟机不再为物理网络所限制。

13.1.7.3 云服务及资源管理层

13.1.7.3.1 IaaS 服务

委 IaaS 服务,提供硬件和软件基础设施服务。具体可包括：云主机与云硬盘,云存储,云网络、云负载均衡、云防火墙和云安全增值服务。

1 ） 云主机和云硬盘服务

云主机功能上支持主流的服务器操作系统,如 Windows Server 系列和主要 Linux 发行版,支持在线交付、在线管理、远程登陆、快照管理、在线迁移等功能。云主机根据业务系统的负载量可提供不同的配置模板,如基础型云主机（1 个 vCPU,2G 内存） 可部署桌面级应用及基础架构类应用,如 Word、浏览器、DNS、MS AD 等； 标准型云主机（2 个 vCPU,4G 内存） 可部署 Web Server,文件服务等； 大内存型（4 个 vCPU,8G 或 1 2G 内存） 云主机可部署邮件系统、应用服务器、轻量级数据库应用等； 高计算型云主机（8 个 vCPU,1 6G 内存） 可部署高性能数据库、数据仓库等。除了以上标准标准配置以外，还支持用户根据业务性能要求自定制配置。云主机系统盘默认配置容量为：Linux 系统盘 20G； 云主机 Windows 系统盘 40G。

云主机通过集群技术保障高可用,当云主机所在的物理服务器故障时,可快速切换到其他状态正常的服务器上,切换时间小于 30 分钟。通过动态资源调度技术自动进行负载均衡,云主机可在线自动迁移到其他物理服务器上,期间应用不会产生任何影响。

云硬盘提供云主机数据盘,单独选配,以 100GB 为最小单位增加。

云硬盘以分布式存储 vStor 作为载体,在 2.2.2 章节已有详细阐述。

云硬盘设置 2 份数据副本同时在线,保障数据高可靠,使得数据持久性大于 99.99%。同时 vStor 支持快照功能,可对云硬盘任一时刻的数据进行快照,含快照制作,快照回滚,快照恢复等。

2) 云存储服务

支持集群技术和分布式文件系统,提供对象存储服务。对于对象存储来讲,不光是解决了数据存储的问题,同时它还解决了数据安全性的问题。存储通常已经依赖于客户端和私有网络的认证来保护系统的安全性,不管在文件服务器内用的是 FCSAN 或 SCSI 阵列。对象存储体系结构在每一个级别上都提供了安全性:存储系统对存储设备的认证; 存储系统对计算节点的认证; 存储系统对计算节点命令的认证;

所有命令都经 CRC 的完整性检查; 数据和命令经由 IP 的私有性。这样的安全水平使得租户可以用更经济高效,可管理并容易访问的 IP 网络,作为存储的传输工具,同时还提高了整个存储体系的安全性。

3) 云网络

云网络支持虚拟交换网络,支持子网划分,支持通过专线或者虚拟专网连接,提供配置管理界面。虚拟交换网络能够监控云主机的流量,针对云主机下发网络策略,且云主机迁移时网络策略能够自动化同步跟随。

4) 云负载均衡

云负载均衡支持将网络请求动态分流到多个云服务器上,支持四层、七层负载均衡,支持对云主机的健康检查,支持用户自行申请开通配置。

5) 云安全服务

提供云防火墙功能,能够支持组建安全组或安全域,对其访问权限进行控制,支持用户自主申请防火墙并灵活配置访问策略。此外, 还提供安全增值服务:如防 DDos 攻击和入侵防御以及日志审计。

IaaS 可为上层的 PaaS 平台提供 API 接口。使得上层的 PaaS 环境可以按需扩展基础设施资源。

13.1.7.3.2 PaaS 服务

PaaS 服务以开发者为核心,平台用户可以在上面开发、测试和部署软件。这意味着,软件的整个生命周期都可以在 PaaS 上完成。

这种服务模式专门面向应用程序的开发人员、测试人员、部署人员和管理人员。

政务专有云平台服务 PaaS 实现了应用开发角度的资源抽象化。

在建设 PaaS 平台的时候,将信息系统中的重要功能中间件,如远程过程调用、数据库代理、消息处理、对象请求代理、事物处理、工作流和地理信息等,纳入到一个集中的,面向服务架构的平台上,形成可以复用的服务构件。应用提供商可以在 PaaS 平台上为各政府部门创建各自独立的用户域,每个用户域可以选取各自不同的软硬件服务平台,并按照自己独有的业务环境和模式来组织这些服

务。所有的信息化系统可通过 PaaS 平台聚合成一个有机的整体。

13.1.7.3.3 多租户组织架构

组织架构定义是云平台的基础,几乎所有的云平台需求都涉及用户和组织关系,这里牵涉到适应政府租户不同的定制需求。云平台支持定制多级组织嵌套,每级组织都会划分自己的资源（CPU、内存、存储、网络等） 和用户。

提供了多种用户的角色,功能视角也不同。iMC 运维管理人员专注于对池化资源的部署分发、服务编排、应用监控,定制流程和计费模板。政府的领导或者 IT 主管作为私有云（或私有云下某个组织）的管理员,关注云容量的规划、服务的质量评价、计费营账报表以及绩效考核等。对于终端用户,更关心 vDC（虚拟数据中心） 服务的申请、流程审批、工单问答以及实时账单等。

用户通过网络进行二层隔离,每个网络都设定了 V(x)LAN 标识和 IP 地址池规划。用户可以使用多个网络以支持不同场景的业务和隔离需求。

13.1.7.3.4 委办局云服务使用流程

除了传统的购买单个主机 vHost、单个应用 vApp 功能外,智能云平台重点体现的是定制 vDC 服务。通过服务 编排打通端网云,生成以应用为中心的虚拟数据中心服务模板,用户仿佛置身于完全属于自己的机房中,对服务的生命周期进行管理。

在自己的 vDC 中,用户可以定制（IaaS 层） 主机、存储服务，通过关联 vLB 来实现负载均衡;申请（PaaS 层） 不同型号的数据库服务,与主机对接； 同时选择云平台提供的应用蓝本定制需要的 （SaaS 层） 软件/应用服务。在网络安全方面,用户可以自主的规划私网网段,设定 vFW 的域间策略实现防火墙安全隔离,甚至可以为应用申请公网 IP ,支持互联网外对服务的使用。用户无须关心如何打通网络（云平台会自动部署） ,只需关注服务本身,通过云平台统一界面实现服务的操作和访问,仿佛机器就摆在眼前； 甚至还能从云平台获取服务的监控统计数据,时刻关注服务的质量。

13.1.7.3.5 云服务的申请与审批

审批是所有政府机构最常见的流程,同时也是个性化最强的业务,需要让云平台服务申请的审批能适应不同政府部门的需要。智能 SOM 服务流程管理工具将审批定义为包含多个有序任务的流。可以定制不同的流程模板,模板支持多级审批,可以定制个性化的审批页面，最大程度满足用户的定制化需求。用户可以将模板与对应的审批流程绑定,不同的审批可以绑定不同的定制流程。

13.1.7.3.6 云服务交付

云主机服务交付

云主机服务是智慧园区大数据云计算在基础设施应用上的重要组成部分。智慧园区大数据云主机服务可让租户完全控制计算资源，当租户的计算资源需求发生改变时，可以通过门户随时进行计算资源的调整。云主机服务整合了常用的管理功能，通过云平台门户租户可以看到他所租用的云主机的配置信息，而且可以对云主机服务执行重启、关机、启动、销毁、调整配置、远程连接等操作。支持随时查看最近八小时、最近一天、最近两周、最近一月 和最近半年云主机服务的监控信息，监控信息包括：CPU 利用率、内存利用率、磁盘 IO 和网络流量。

云主机概述

云主机是整合了计算、存储与网络资源的 IT 基础设施能力租用服务，能提供基于云计算模式的按需使用和按需付费能力的服务器租用服务。客户可以通过 web 界面的自助服务平台，部署所需的服务器环境。

云主机是一种可随需获取的弹性计算资源，可以视为一台预配好的服务器，包含了硬件配置、操作系统以及网络配置。基于主机资源，可构建各种应用服务。

云主机的功能包括：租户的云主机列表、创建云主机、云主机的操作列表、云主机的监控信息和费用报告。

1 、云主机的列表：租户以 Web 方式登录 XXXloud 云服务管理平台后，可以查看所有自己管理的主机列表，查看云主机信息包括：所属用户、名称、状态、内网 IP、镜像模板、规格类型、网络、运行时间和远程登录主机；

2、创建云主机：根据镜像的分类选择镜像，镜像列表包括镜像名称和描述；

3、创建云主机：选择规格，规格内容包括规格类型、CPU、内存和系统盘； 配置详情包括每小时和每天的总价：

4、创建云主机：设置网络，选择云主机接入的网络；

5、创建云主机：基本配置，需要输入云主机名称、云主机数量和描述；

6、当云主机创建完毕以后，云主机操作列表，租户拥有所有权限，具有完全的控制权，可以管理所有的主机操作，包括刷新、新建、启动、关机、重启、修改等； 就像操作物理服务器一样。

7、租户可以查看云主机的监控信息，并可以查看包括所有的费用总统计和明细、资源总统计和明细，应用统计和性能统计

自定义镜像

自定义镜像是针对有效运行云服务器的用户，通过已创建的自定义镜像，可一次性开通多台已完全拷贝相同操作系统及应用环境和数据的云服务器，以便满足弹性扩容的业务需求。

镜像模板是带有操作系统的主机模板。除了系统提供的标准 Linux 、Windows 模板外，租户可以将自己名下的云主机制作成模板，以备后用。

创建主机时可以从镜像模板中选择；

1 、镜像模板列表，包含两部分，一部分为系统自定义的，不能修改和删除，另一部分为自由的镜像模板，可以创建、修改和删除。

2、创建镜像：只能从自由列表中创建镜像模板，包括名称、描述、类型、格式化、最小磁盘和

最小内存等。

云主机标准配置

云主机模板按照云主机的 vCPU、内存等参数,根据业务系统负载量的不同提供不同的规格,下表为部分典型云主机配置（Windows 云主机免费提供 40G 系统盘,Linux 云主机免费提供 20G 系统盘） 。

除此之外,还可根据业务需要对云主机自定义配置。云主机可挂载云硬盘作为数据盘,可选范围为 1 0GB-500G。B 计费项（操作系统、CPU、内存）

1 2GB 一核

2 4GB

3 4GB 两核

4 8GB

5 云主机及操

6 作系统 四核

8GB

1 2GB

7 1 6GB

8 1 6GB

9 八核 24GB

1 0 32GB

云硬盘

云硬盘提供云主机数据盘,单独选配,可以 1 0GB 为最小单位增加,租户可申请云硬盘直接挂载到云主机上。它独立于主机的生命周期而存在,可以被连接到任意运行中的主机上,为主机提供持久化的、块级存储,并可以随时解除连接,转接至其他主机,如此可以实现数据的快速转移。云硬盘以分布式存储 vStor 作为载体,在 5.2.2 章节已有详细阐述。云硬盘设置 2 份数据副本同时在线,保障数据高可靠,使得数据持久性大于 99.999%。同时 vStor 支持快照功能,可对云硬盘任一时刻的数据进行快照,含快照制作,快照回滚,快照恢复等。

云硬盘申请流程如下：

申请云硬盘,包括名称、描述、数量和容量（1 00GB）;

云硬盘列表和云硬盘操作列表,操作列表包括加载到主机、卸载硬盘、扩容和销毁。

将云硬盘挂载到主机云硬盘的详细信息、租用信息和监控信息云主机特点全 Web 化管理：租户通过自助服务界面申请和管理云主机。租户拥有云主机的所有权限,可像操作物理服务器一样控制云主机。

快速供应：云平台计算资源池内置多种云主机标准镜像,可按需选择操作系统,待审批通过以后可实现快速供应,从创建到启动在 5 分钟以内。

高可用性：通过虚拟化集群方案、动态资源调度以及热迁移技术，结合分布式存储技术的高可

用性,实现云主机可用性大于等于 99.9%。

云主机在线迁移：借助动态资源调度特性,云平台可根据物理主机负载情况综合调度,将云主机在不停机状态下从一台物理主机迁移到另外一台物理主机； 在线迁移时,云主机应用完全不中断,用户完全无感知。

云主机克隆：支持对云主机克隆,根据云主机数据盘的大小整个克隆过程一般在 1 5 分钟以内。

云主机升级。当云主机现有配置不满足要求时,用户可自主进行云主机配置快速升级,可升级配置包括：CPU,内存,网络带宽等；配置升级生效时间在 1 0 分钟以内。

弹性：保护租户投资且无需对系统、环境和数据做任何变更,租户可按需求动态的创建和分配计算、存储、网络带宽等资源； 租户可以在线按时长购买云主机,并支持任意时刻的续费管理。

云存储服务交付

云存储产品随着云计算的落地,已经得到了诸多厂商的支持和关注,云存储是在云计算概念上衍生和发展出来的一种新的技术或者服务,云计算是将分布式处理、并行处理、网络计算相互结合,通过网络将计算机处理程序自动分拆成无 数个较小的子程序再由多部服务器组成的庞大系统经计算分析之后将结果交回给用户。云存储则是将网络中各类存储设备通过应用软件集合起来协同工作,对外提供数据存储和业务访问功能的一个系统。

云存储通过对象存储形式提供服务。对象存储是 块设备,文件系统之后最近兴起的一种存储格式。对象存储具有很多先进的特性：

1) 建立在分布式架构之上,可用性大于等于 99.9%,数据持久性大于等于 99.99999999%

2) 根据系统实际情况,方案可灵活支撑系统扩容。扩容包括 3 方面：流数据扩容、元数据扩容、业务系统扩容； 无文件数量限制

3) 支持部署 MySql 数据库,单库容量达 1 TB

4) 支持部署 Hbase,单表存储空间达 1 OOTB

5) 支持文档、视频、音频、图片等类型的对象存储。文件大小可达 5TB

6) 通过分布式存储技术实现 2 份副本,单台服务器故障不会导致数据丢失。

云存储的控制台通过 Web 方式登录,支持 IE8+、Firefox 、Chrome 等浏览器,可通过 Web 页面实现文件的读、写、删、查以及复制功能。

针对大文件以 4mb 为单位分块上传,上传到服务器上进行合并处理，降低了服务器中存放块的数量,同时也方便下载大文件； 上传和下载均支持断点续传。云存储为用户提供丰富的插件,帮助客户自身情况更好配置整个系统。云存储提供完整的 API 接口,帮助与第 3 方系统整合。提供的是标准的 RestFul 类型接口,同时提供 Java、Python 、Object-c 二次开发包。

云存储的安全通过以下三种方式实现：

1) 可记录和查询管理员和用户的访问日志信息,包括上传、下载、目录管理等。可按多种条件进行统计查询。

2) Hmac 加密算法可以有效地保证用户的请求不被篡改,加上时间戳等信息,可以避免外 被非法引用。

3) 通过 SSL 安全通道保障数据传输安全。可通过 MD5 加密存放数据。

云网络服务交付

云主机租户网络能够快速搭建您的私有云环境,并使用丰富的工具进行自动化管理。私有网络间使用路由器互联,并可与公网 IP 绑定。最后只需将主机加入网络即可。

私有网络

私有网络用于主机之间的互联,它类似于物理世界中使用交换机（L2 Swirch ） 组成的局域网。与基础网络相比,私有网络提供 1 OO%隔离。

1 、创建网络,输入网络名称和描述信息：

2、配置网络,在这里我们可以查看和修改私有网络包含的主机列表和端口列表；

路由器用于私有网络之间的互联,并提供以下附加服务：DHCP 服务、端口转发、隧道和 VPN。如果您还希望路由器能接入互联网，请绑定一个公网 IP 给该路由器即可。

1 、云管理服务台支持创建路由器；

2、配置路由器,可以配置基本信息和租户信息：

3、路由器列表和操作列表,包括 ID、名称、状态、私网 IP 、描述和创建时间等：

云安全服务交付

云安全服务包括云防火墙服务和安全增值服务,包括流量清洗、入侵防御和安全日志审计服务。

云防火墙服务是提供给租户在申请云主机、云存储等服务时配套提供的安全防护服务,以满足租户个性化的安全防护需求,如实现不同业务系统之间的隔离。租户可以通过服务门户申请云防火墙资源。

在满足需求的前提下,同时达到可运维、可管理的目的。

平台出口交换机上,作为增值安全服务提供给租户,提供入侵防御 /检测、病毒过滤和带宽管理等功能； 通过在云系统管理区部署安全日志审计服务器,对日常收到的攻击、威胁等日志信息进行采集和分析。

云负载均衡服务交付

为了应对 Web 类应用流量不断增长的态势,另外一方面,业务系统的高可用需要防范 Web 前端服务器的单点故障,借助负载均衡技术实现服务器负载均衡是一个目前为业界广泛采用的解决方案。负载均衡可以实现对网络设备和服务器带宽的有效扩展,充分利用多台服务器的业务处理能力,通过合理的调度算法和健康检查双方,可以有效感知服务器的负载并将业务流量调度到最恰当的服务器上,从而提高网络的灵活性和可用性。

政务外网云服务平台可以为政务用户提供云负载均衡服务。

在申请云负载均衡时,租户可以根据自身需要,配置 vLB 的指标参数,如 vLB 数量、吞吐量、服务 IP 地址等,满足用户 vDC 自定义的需求。

云负载均衡与云防火墙一样,也是属于云主机的配套服务。租户可根据自身业务系统的需要,如吞吐量、业务类型、负载均衡方式等选择合理的负载均衡策略。

云负载均衡具备以下特点：

1）可提供 4-7 层的负载均衡,包括 HTTP、IP 、TCP 和 UDP 等协议类型。对 Web 和应用服务器,可透明接入。

2）可以按照指定规则进行健康检查,自动隔离异常状态云主机,迅速实现服务切换,切换时间为秒级。

3）可以将用户和后台服务器绑定到同一会话,确保会话不中断。其中 4 层负载均衡可以设置连接持久时间。

4）提供 API 或控制台调用方式,可以随时开启,关闭负载均衡， 立即生效,灵活简单。

5）支持按使用时间进行计费。

6）采用分布式结构,具有高度的冗余和可靠性,可根据系统负载弹性扩容。

7）可根据后台云服务器的性能设置不同的转发权重,权重支持轮询,最小连接数转发等方式。

云数据库服务交付

云数据库提供 MySQ、L MS SQLServer 或者 Oracle 数据库服务。

MySQL 可提供 5.1 ,5.5 或 5.6 版本,MSSQLServer 可提供 ***8 版本。

云数据库服务便捷易用,一键搞定 ； 多维度监控,全方位保证安全 ；

性能卓越,专业团队承诺。

目前可提供如下不同性能规格的云数据库服务目录：

云数据库服务监控

通过平台监控功能实现对实例级别在不同时间粒度完成对磁盘空间、连接数、CPU、内存、网络流量等参数的监控数据展示云数据库功能及特性：

1）支持关系型数据库的管理、数据库操作、备份、迁移等基本功能。提供多重备份功能,可从备份文件创建临时数据库,也可恢复到生产环境。支持数据导入、导出工具,方便用户进行数据迁移。

2）MsSqlserver 单数据库实例可创建的数据库数量达 20 个,用户数达 20 个。

3）Mysql 单数据库实例可创建的数据库数量达 *** 个,用户数达 50 个。

4）服务便捷易用,通过 Web 自助门口快速获取数据库服务。按需开通,即开即用,按需计费。随着用户数和访问量的变化,可以弹性的调整数据库的规格,包含内存、连接数、IOPS、存储容量等,调整时服务不间断。

5）可提供 API 接口、SDK 开发包 ， 方便用户进行集成开发。

6）提供日志记录功能,包括错误日志、操作日志、访问日志等,可按访问来源进行多维度的统计分析。

7）高可用,通过数据库集群技术,存储的冗余备份、全方位监控保障可用性大于等于 99.95%。通过 HA 技术实现数据库在线升级、云内动态迁移、故障自动切换,实现业务秒级无缝切换,不中断用户服务。

8）云数据库采用高性能高可靠 FC 存储,数据持久性大于等于 99.9999%,存储 IOPS 性能超过 13000。物理磁盘采用 Raid1 0，任何时刻都有两份数据副本,一份数据丢失,服务会自动切换，不会对造成任何中断影响。单数据库实例内存可达 32G,并发连接数可达 ***0 以上。

9）高安全性,支持 IP 授权访问,支持加密用户身份验证,支持访问权限控制。支持数据库存储加密。

13.1.7.4 vDC 虚拟数据中心

高

13.1.7.4 vDC 虚拟数据中心

高

13.1.7.4 vDC 虚拟数据中心

高

13.1.7.4 vDC 虚拟数据中心

高

13.1.7.4 vDC 虚拟数据中心

高

13.1.7.4 vDC 虚拟数据中心

高

13.1.7.4 vDC 虚拟数据中心

高

13.1.7.4 vDC 虚拟数据中心

高

13.1.7.4 vDC 虚拟数据中心

高

13.1.7.4 vDC 虚拟数据中心

随着虚拟化与云计算技术的不断成熟,越来越多的云服务提供商(如:Amazon EC2 、HP Cloud 等)开始提供公有云服务,允许租户按需租用资源和服务,创建租户自己的虚拟数据中心(vDC,VirtualData Center) 或虚拟私有云(VPC,Virtual Private Cloud),帮助租户节省建设成本、提高业务敏捷性。因此,云服务商平台需要考虑为各委办局或其他用户提供服务,帮助用户将大部分 IT 应用向智慧园区大数据云迁移。政务外网云平台为租户(委办局单位) 提供云主机、云存储、云网络安全等虚拟基础设施资源,基于这些虚拟资源,租户可以在专有云中构建自己的虚拟数据中心,同时各租户的虚拟数据中心彼此安全隔离。

虚拟数据中心(vDC) 的最大好处就是可以让租户灵活部署自己的业务应用,就像部署在自己的专属数据中心内部,拥有计算、存储和网络虚拟实例完整的使用权和管理权。

对于计算、存储资源的虚拟化,目前的技术成熟度很高,使用也非常普遍。然而对于网络安全资源的虚拟化技术实现,是构建虚拟数据中心的重点和难点,XXX 通过多年在网络安全领域的积累,很好的将网络安全的虚拟化技术应用到了 XXXLOU 云 D 平台中,通过硬件设备的 1:N 虚拟化和 NFV(网络功能虚拟化) 技术,实现网络安全资源虚拟化。

由于布线、归属等原因,目前的物理设备并不适合作为租户独享的设备在云计算环境中部署。为了解决目前存在的问题,需要一个既具备物理网络设备的功能又适合于在公有云多租户环境中部署的设备,NFV(Network Function Virtualisation, 网络功能虚拟化) 应用而生。

XXX 提供一系列 NFV 方案,应用于 vDC 场景,帮助政务外网云平台构建租户的私有云或混合云。它和物理设备一样,采用业界领先的专业网络平台 Comware V7,运行在标准 X86 服务器或虚拟机上,提供和物理设备相同的功能和体验,包括路由、防火墙、VPN、QoS、及配置管理等,同时充分利用虚拟平台的特点,简化设备的部署安装。

领先的专业网络平台

基于业界领先的 Comware V7 平台,支持:

丰富的网络和安全功能,能够满足政府分支及专有云多租户环境中的网络需求。

控制平面和数据平面分离,专门为虚拟环境优化的多核数据转发,更能充分利用计算资源。

模块化的体系架构,开放的网络平台,允许网络按需运行和控制, 更容易实现 NFV/SDN 落地。

和物理网络设备采用统一的软件平台,提供相同的功能特性和一致的管理界面。

超轻量级部署

XXX NFV 提供了超轻量级的部署体验:

适合在私有云中部署,实现零运输、零布线,加快业务的部署。

支持 VMware ESXi、Linux KVM、XXX CAS 等多个主流的虚拟平台,充分发挥虚拟化的优势,实现快速部署、批量部署、镜像备份、快速恢复,并且能够灵活迁移。

提供 ISO 镜像、OVA 模板、IPE 等多种发布格式,适应各种环境下的部署。

支持虚拟机管理平台、网管平台及本地等多种工具进行灵活部署。

超强业务弹性

支持 VMware ESXi、Linux KVM、XXX CAS 等多个主流的虚拟平台,无缝适应用户的部署环境。

允许政务外网云平台在虚拟化的环境中搭建政府网络,可以按需动态地调配和管理网络资源及服务,比如,可以很方便的通过配置对 VSR、VFW、VLB 的网口数量和类型进行灵活调整,而无需新购买硬件板卡。

通过动态调整虚拟机资源和 License ,即可实现网络功能的平滑升级、设备性能的按需提升,随时满足业务增长需求。

扩展委办局网络到云端

租户在专有云中部署 NFV,能够实现:

将租户 VPC 网络作为政府网络的一部分进行管理,确保一致的网络配置、安全策略、管理策略、及 IP 地址规划等,实现统一的政府网络管理。

和分支一样,实施统一的流量控制、部署一致的网络业务(如:QoS、防火墙、负载均衡、WAN 优化等) ,提供一致的网络业务体验。

在智慧园区大数据云和委办局之间建立端到端的 VPN 连接,使得专有云应用访问更安全,同时端到端的访问避免了总部中转,减少了云应用的响应时间,提高了云应用的使用体验。

XXX VSR 作为 vDC VPN 网关

在智慧园区大数据云中,数据中心对服务器资源进行统一管理,分配给委办局进行应用安装和数据保存,部门之间的安全隔离是首要需求,同时会有一些信息共享和数据互访需求,另外,政务用户还可以根据需要访问各个部门的数据。

VSR 作为 VPN 网关部署在数据中心,提供:

部门间的数据隔离和共享控制。

部门人员、领导通过 VPN 可安全访问各部门的数据。

VSR 作为接入网关部署在部门。

网关接入、VPN 安全等功能。

vCPE 提供虚拟化平台,除运行 VSR 外,还能很方便地集成其他业务应用。

XXX VFW 作为 vDC 安全隔离网关

XXX VFW 提供和物理设备同样的安全特性,包括 :

支持包过滤。借助报文中优先级、TOS、UDP 或 TCP 端口等信息作为过滤参考,通过在接口输入或输出方向上使用标准或扩展访问控制规则,可以实现对数据包的过滤。同时,还可以按照时间段 进行过滤。

支持应用层状态包过滤(ASPF) 功能。通过检查应用层协议信息(如 FTP、HTTP、SMTP 、RTSP

及其它基于 TCP/UDP 协议的应用层协议） ,并监控基于连接的应用层协议状态,动态的决定数据包是被允许通过防火墙或者是被丢弃。

支持丰富的攻击防范技术。包括：Land、Smurf、Fraggle 、Ping ofDeath、Tear Drop、IP Spoofing 、IP 分片报文、ARP 欺骗、ARP 主动反向查询、TCP 报文标志位不合法超大 ICMP 报文、地址扫描、端口扫描等攻击防范,还包括针 SYN Flood、UDP Flood、ICMP Flood 等常见 DDoS 攻击的检测防御。

支持多种 VPN 业务,如 L2TP VPN、IPSec VPN、GRE VPN 等,可以针对客户需求通过拨号、租用线及 VLAN 或隧道等方式接入远端用户,构建 Internet 、Intranet 、Access 等多种形式的 VPN。

结合防火墙、AAA、NAT、及多种 QoS 等技术,防火墙可以确保在开放的 Internet 上实现安全的、满足可靠质量要求的私有网络。

支持安全市域管理。可基于接口、VLAN 划分安全市域。

支持静态和动态黑名单。

支持丰富的路由协议。支持静态路由、策略路由,以及 RIP、OSPF 等动态路由协议。

NAT 应用及 VPN 接入能力。

在智慧园区大数据云中,VFW 作为出口网关,防范各种来自外部的攻击,也可作为内网访问控制设备隔离不同安全等级的区域,实现对网络流量的安全防护。

精简网络基础设施,直接利用服务器,便于租户自行维护；

业务弹性扩展,性能可动态调整,管理高效

支持分区域安全控制

支持 NAT,支持多种 ALG

通过报文检测并阻止非法入侵。

支持多种攻击防范技术。

支持黑名单过滤。

支持通过 TCP 代理实现 Syn Flood 防攻击。

支持流量日志及攻击告警日志。

XXX VLB 作为 vDC 多租户负载均衡应用

在智慧园区大数据云环境中,为了实现对租户应用服务的快速访问,也需要采用应用交付功能来分担和优化租户应用的访问流量。在这种情况下,可以为不同租户部署专用的 VLB 产品,提供负载均衡功能,保证租户服务的响应速度和业务连续性,提高应用可靠性； 同时也可以与 VFW 配合使用,支持与 VFW 在相同的物理服务器上部署；

精简网络基础设施,直接利用服务器,便于租户自行维护；

业务弹性扩展,性能可动态调整,管理高效

支持 4-7 层服务器负载均衡；

支持丰富的负载均衡调度算法；

支持高效的健康检查算法；

支持多种攻击防范技术。

13.1.8 互联网云平台架构

无论是 xxx 网云平台和电子政务互联网云平台其整体架构是相同的。不同之处在于计算资源容量和安全防护能力的不同。

互联网业务区提供完备的安全保护措施,除配置与 xxx 网相同的 FW、IPS、SSLVPN、数据库审计、堡垒机、漏洞扫描、安全管理中心以及安全资源池的 vFW、vLB,另外配置了 DDoS 、行为审计、网页防篡改、WA、F 硬件负载均衡、安全管理检测中心等。

1 、DDOS 流量清洗：对进入云平台的数据流量进行实时监控,及时发现包括 DOS 攻击在内的异常流量。在不影响正常业务的前提下，清洗掉异常流量。有效满足用户对云平台运作连续性的要求。同时通过时间通告、分析报表等服务内容提升用户网络流量的可见性和安全状况的清晰性。

2、行为审计：对网络中的 P2P/IM 带宽滥用、网络游戏、炒股、网络视频、网络多媒体、非法网站访问等行为进行精细化识别和控制,保障网络关键应用和服务的带宽,对网络流量、用户上网行为进行深入分析与全面的审计,进而帮助用户全面了解网络应用模型和流量趋势,优化其带宽资源,开展各项业务提供有力的支撑。

3、网页防篡改：专注于网站内容安全,可以为网站提供不间断的监控与保护,有效的保障网站的完整性和真实性。

4、WAF ：专注于 7 层防护,采用双引擎技术,采用用户行为异常检测引擎、透明代理检测引擎相结合的安全防护机制实现各类 SQL 注入、跨站、挂马、扫描器扫描、敏感信息泄露、盗 行为等攻击防护,并有效防护 0day 攻击,支持网页防篡改。支持 Web 应用加速,支持在透明代理部署模式下的 HA/Bypass,便于部署配置以及维护。可以帮助用户解决目前所面临的各类网站安全问题,如：注入攻击、跨站脚本攻击、恶意编码 （ 网页木马 ）、缓冲区溢出、信息泄露、应用层 DOS/DDO 攻 S 击等。

5、硬件负载均衡：部署在数据中心的核心层,基于特定的负载均衡算法将客户端对数据中心服务的访问请求合理地分发到数据中心的各台服务器上,以保证数据中心的响应速度和业务连续性。实现了应用优化、安全与网络的深度融合，具有强大的路由、交换、负载均衡、2-7 层安全等功能。

6、安全管理检测中心：是一套软件产品,采用远程监测技术对 WEB 应用提供 7*24 小时实时安全监测服务。通过对网站的不间断监测服务从而提升网站的安全防护能力和网站服务质量,并通过安全监测中心的事件跟踪功能建立起一种长效的安全保障机制。为应对当前复杂的网络安全形势,进行以漏洞监测为主的多维度监测。平台的安全监测维度分别为漏洞扫描、网马监测、篡改监测、敏感关键字监测、可用性监测,围绕着任务集中管理,形成 7*24 小时的实时监测。

13.1.9 云平台部署逻辑架构

在网络系统设计中,从上图可以看出,xxx 网云平台和电子政务互联网云平台各自具备一套云管理平台,云平台管理网络和业务网络属于两套分离的网络系统。并且 xxx 网云平台和电子政务互联网云平台各自有独立的业务网络系统。

在计算资源设计中,xxx 网云平台和电子政务互联网云平台各自使用物理隔离的计算资源,并且在同一个云平台下的计算资源中,依据承载业务业务应用系统信息安全等级保护级别的不同,在物理上分离的划分出了二级等保计算资源区和三级等保计算资源区。

13.2 IaaS 层方案

13.2.1 网络虚拟化

13.2.1.1 基本需求

为了满足本次的 XX 市智慧园区大数据云的项目 业务实际需求，在业务承载的基础网络部分也衍生出如下几个基本的需求：

1. 首先需要满足在云环境下能够为智慧园区大数据云下的各种业务隔离； 智慧园区大数据云是为各单位共同接入的公共平台，从安全性的角度考虑,各单位之间以及单位内各业务系统需要实现相互隔离。

2. 其次在云环境下,最大的好处在于计算资源能够随需移动,计算资源通过计算虚拟化可以实现在单台的物理机下虚拟化成多个虚机,为了保障业务快速部署,业务的高可靠性,各虚机需要在各租户网络内部进行迁移,或进行集群,虚机迁移,其 IP 地址和 IP 网关本身不会变化,同时虚机集群也需要各虚机保持在一个网段之内,所以从整个基础网络来看,需要整个数据中心需要提供一个大二层网络。

3. 从整个 XX 智慧园区大数据云的建设情况,其接入单位众多,业务需求多样； 各单位后续的业务规模难以准确预测,需要基础网络具备灵活的弹性,能够满足在后期业务的弹性扩展,包括单一业务的规模扩展,单一用户的规模扩展； 扩展范围甚至覆盖到另外区域的数据中心。

13.2.1.2 技术选择

根据上述的几个需求来看,XX 市智慧园区大数据云数据中心建设,必须要满足多租户安全接入,租户内部网络隔离,实现各局存在的相同 IP 地址段的平滑接入,简单的大二层,后续弹性扩展等多

个需求。针对当前常见的数据中心技术进行具体分析：

VLAN+STP 技术

传统的核心、汇聚、接入通过 VLAN 实现租户的隔离,通过 STP 实现多路径保护； 但传统二层网络中部署的 STP 生成树技术协议,部署和维护繁琐,网络规模不宜过大,限制了网络的扩展。而后以厂家私有网络虚拟化技术如 vPC 等网络虚拟化技术,虽然可以简化部署、同时具备高可靠性,但是对于网络的拓扑架构有严格要求,同时各厂家不支持互通,在网络的可扩展性上有所欠缺,只适合小规模网络部署,一般只适合数据中心内部网络； 此外云业务中虚拟机的大规模部署带来的另一个问题就是使传统网络设备二层地址（MAC ） 表项的大小成了云计算环境下虚拟机规模的关键参数,特别是对于接入设备而言,二层地址表项规格较小,这也将限制整个云计算数据中心业务规模； 不建议在此次项目中采用。

TRILL/SPB/FabricPath+VLAN

随着数据中心接入规模的要求,新出现了大规模二层网络技术 TRILL/SPB/FabricPath 等,它们通过引入 ISIS 等协议实现多个二层网络的互通,能支持二层网络的良好扩展,但对数据包所经过的沿途所有网络设备有特殊要求,网络中的设备需要软硬件升级才能支持此类新技术,带来部署成本的上升,同时各厂商互通成为一个难以解决的问题,由于采用传统的 VLAN 接入,随着智慧园区大数据云业务的快速发展,对于租户的数量可能在不远的将来成为制约智慧园区大数据云向更多规模扩展的瓶颈,因此本次需要寻求更具弹性的网络技术实现智慧园区大数据云的接入。

SDN+Overlay 的网络虚拟化技术

Overlay 技术是专门针对多租户数据中心建设而引入的技术,在业界知名的互联网数据中心中,以及公有云的建设中成为当前基础网络的首选技术,Ovelay 是一种网络架构上叠加的虚拟化技术模式，其大体框架是对基础网络不进行大规模修改的条件下,实现应用在网络上的承载,并能与其它网络业务分离,并且以基于 IP 的基础网络技术为主。

Overlay 网络是指建立在已有网络上的虚拟网,逻辑节点和逻辑 路构成了 Overlay 网络。

Overlay 网络是具有独立的控制和转发平面,对于连接在 overlay 边缘设备之外的终端系统来说,物理网络是透明的。

Overlay 网络是物理网络向云和虚拟化的深度延伸,使云资源池化能力可以摆脱物理网络的重重限制,是实现云网融合的关键。

Overlay 网络概念图

从当前业界的应用情况来看,Overlay 可以满足 XX 智慧园区大数据云对于多租户接入、多租户隔离、弹性扩展、大二层组网等需求，建议本次 XX 智慧园区大数据云采用 Overlay 技术实现整个基础网络的构建。

13.2.1.3 模型选择

Overlay 技术介绍及选择

IETF 在 Overlay 技术领域提出三大技术方案：

VXLAN：VXLAN 是将以太网报文封装成 UDP 报文进行隧道传输，UDP 目的端口为已知端口,源端口可按流分配,标准 5 元组方式有利于在 IP 网络转发过程中进行负载分担； 隔离标识采用 24 比特来表示；未知目的、广播、组播等网络流量均被封装为组播转发。

NVGR：E NVGRE 采用的是 RFC2784 和 RFC2890 所定义的 GRE 隧道协议。将以太网报文封装在 GRE 内进行隧道传输。隔离标识采用 24 比特来表示； 与 VXLAN 的主要区别在对流量的负载分担上,因为使用了 GRE 隧道封装,NVGRE 使用了 GRE 扩展字段 flowID 进行流量负载分担,这就要求物理网络能够识别 GRE 隧道的扩展信息。

STT：STT 是无状态传输协议,通过将以太网报文封装成 TCP 报文进行隧道传输,隔离标识采用 64 比特来表示。与 VXLAN 和 NVGRE 的主要区别是在隧道封装格式使用了无状态 TCP,需要对传统 TCP 协议进行修改以适应 NVGRE 的传输。

总体比较,VXLAN 技术具有最佳优势：

1) L2-4 层 路 HASH 能力强,不需要对现有网络改造 （GRE 有不足,需要网络设备支持）

2) 对传输层无修改,使用标准的 UDP 传输流量（STT 需要修改 TCP）

3) 业界支持度最好,商用网络芯片大部分支持基于此,本次的 XX 市智慧园区大数据云方案建议选择基于 Vxlan 的 Overlay 技术实现本次方案的建设。

SDN 技术的引入

上面提到了 Overlay 的转发层面,在 Overlay 的控制层面,传统的 Overlay 各 VETP 节点之间需要通过主机虚机的 MAC 地址需要部署 IP 多播路由协议,且需要支持任意源（ASM） 模式——每个成员既是多播的接收者,又是多播的发起者。这大大增加了网络运维的难度。

一方面物理网络支持的 IP 多播组数量是有限的,远小于 VXLAN 虚拟网络的个数,这限制了整个 VXLAN 网络的租户数量； 另一方面每个 IP 多播组中的成员个数也是有限的,此外对于多播网络的维护也是一个复杂的过程,因此在本次提供的方案中,将采用 SDN 的技术,通过引入 SDN 控制器,实现 Overlay 控制层面的简化,同时利用 SDN 的服务 的技术,将整个网络的安全业务部署进一步简化,让 Overlay 能够更好的为本次的 XX 智慧园区大数据云提供服务。

Overlay 方案模型介绍及选择

根据客户不同组网需求,Overlay 分为三种组网模型（如图所示） 。

网络 Overlay ：隧道封装在物理交换机完成。这种 Overlay 的优势在于物理网络设备性能转发性能比较高,可以支持非虚拟化的物理服务器之间的组网互通。

主机 Overlay ：隧道封装在 vSwitch 完成,不用增加新的网络设备即可完成 Overlay 部署,可以支持虚拟化的服务器之间的组网互通。

混合 Overlay ：是网络 Overlay 和主机 Overlay 的混合组网，可以支持物理服务器和虚拟服务器之间的组网互通。

三种 Overlay 组网模型

相对于主机 Overlay 和软件网络 Overlay ,混合型 overly 网络解决方案,它具有如下特点：

1 ）Overlay 网络是指在传统网络的边缘构架一套全新的智能控制网络。该网络中的结点可以看作通过虚拟或逻辑 路而连接起来的,在 Overlay 方案中,边缘节点设备可以支持逻辑软件和独立的硬件设备。

2）Overlay 网络具有独立的控制和转发平面,对于连接在 overlay 边缘设备之外的终端系统来说,物理网络是透明的,只需 IP 可达,并且不在完全限定物理网络是二层网络或是三层网络，具有更高的灵活性。

3）Overlay 网络是物理网络向云和虚拟化的深度延伸,使云资源池化能力可以摆脱物理网络的重重限制,是实现云网融合的关键。

4）Overlay 的网络架构是在传统物理网络基础上构建了逻辑的二层网络,是网络支持云业务发展的理想选择,是传统网络向网络虚拟化的深度延伸,提供了网络资源池化的最佳解决方式。

鉴于 XX 市政府各下属单位前期 IT 建设阶段不同,现网存在多种不同类型数据库,支撑不同类型业务,有些关键应用为了保证期高性能和稳定性,目前不建议放在虚拟化环境中,但是依然希望能将其纳入 overlay 网络中统一管理,针对这种情况,混合型 overlay 方案，能够提供一套包含软硬件的整体解决方案,将云数据中心的所有虚拟机和物理服务器（包含虚拟机宿主和独立承载核心业务的物理主机）同时纳入管理,由 SDN 控制器统一控制下发网络策略。Overlay 控制器作网络管理的核心,和计算管理,存储管理模块一起,受云管理平台的统一控制。

13.2.1.4 SDN 网络规划与设计

本次 XX 市智慧园区大数据云整体网络规划建设中,为了达到安全合规性要求,同时提高智慧园区大数据云整体安全性,分别为宏网业务区和互联网业务区建设了一套相互独立的网络系统平台,而 xxx 网业务区和互联网业务区内部核心网络结构是相同的。

1） VCFC Controller 高可用集群架构规划：

智慧园区大数据云业务网络全部运行在 VxLAN 网络中,实现业务网络与物理网络的从逻辑上的分离。而智慧园区大数据云网络整体的运行全部由 VCFCController 网络控制器进行控制,为了保证网络的稳定运行,VCFC Controller 网络控制器采用了分布式高可用集群架构设计。

分别在 A 数据中心、B 数据中心和政府当前数据中心部署 2 台 VCFCController 网络控制器,每个数据中心的两台 VCFCController 网络控制器组成一个 Team 称之为 Region,A 数据中心为 Region1 ,B 数据中 心为 Region2,政府当 前数据中 心为 Region3。Region1 、Region2 和 Region3 组成了分布式高可行 SDN 集群。

Region1 、Region2 和 Region3 所有的 VCFC 控制器只需要 IP 可达即可保持相互之间的必要通讯。

2） VCFC Controller 网络控制器的作用：

可以向防火墙设备、核心交换机设备、接入交换机设备和虚拟交换机设备下发配置信息和流表信息,从而集中控制网络整体的转发策略。

3） VxLAN 三层网关：

核心交换机是智慧园区大数据云 SDN-VxLAN 三层网关,主要实现不同的 VxLAN 之间、不同的 VxLAN 和 VLAN 之间的互通。

数据中心内的 VXLANIP GW 以堆叠的形式部署,两个数据中心的 VXLAN IP GW 堆叠再部署成网关组,以满足业务迁移的要求。

4） 防火墙 - 智慧园区大数据云安全网关

此处的防火墙是智慧园区大数据云安全网关,负责智慧园区大数据云内部业务系统的安全防护,同时提供租户间的安全隔离。

数据中心内的防火墙以堆叠的形式部署,VCFC 集群对不同数据中心的防火墙分别进行安全纳管,可根据业务需要在控制器上直接下发策略,策略会同时在两个数据中心的防火墙下发,以确保虚机迁移后业务不受影响。

5） VxLAN 网络

在改造后的物理网络之上构建一个虚拟网络,上层应用只与虚拟网络相关。Overlay 网络主要由三部分组成：边缘设备、控制平面和转发平面。

边缘设备：与服务器或虚拟机直接相连；

控制平面：负责虚拟隧道的建立维护以及主机可达性信息的通告；

转发平面：承载 Overlay 报文的现有物理网络。

Overlay 架构图

此次所涉及 VXLAN 网络的所有交换机,都支持 VXLAN 报文封装,VXLAN 这种二层 Overlay 技术,将以太网报文承载到某种隧道层面,VXLAN 利用了现有通用的 UDP 传输 VXLAN 运行在 UDP 上,物理网络只要支持 IP 转发,则所有 IP 可达的主机即可构建一个大范围二层网络。屏蔽了物理网络的模型与拓扑差异,将物理网络的技术实现与计算虚拟化的关键要求分离开来,几乎可以支持以太网在任意网络上的透传,使得云的计算资源调度范围空前扩大。

13.2.1.5 Overlay 网络介绍

本次针对 XX 智慧园区大数据云提供的网络虚拟化方案：本次方案中采用 XXX 的混合 Overlay 技术实现基础网络搭建,针对有虚拟化的主机,提供 VSW 实现虚机的 Overlay 接入,未做或不能做虚拟化的主机,通过 L2 层网关实现接入； 为了简化 Overlay 网络的部署,引入 SDN 控制器 VCF Controller ,实现 Overlay 的流表学习和控制； 为了更灵活地针对各虚机、业务、以及租户的安全控制， 引入 SDN 的服务 的技术,通过 L2 网关实现接入安全资源池的接入。

该组网方案有以下优点：

适用于服务器虚拟化的场景,成本较低,VXLAN 物理 GW 既可以用在核心位置,也可以在现有核心旁挂,保护已有投资。

控制面实现可以由 XXX 高可靠的 SDN Controller 集群实现， 提高了可靠性和可扩展性,避免

了大规模的复杂部署。

网关组部署可以实现流量的负载分担和高可靠性传输。

支持分布式网关功能,使虚机迁移后不需要重新配置网关等网络参数,部署简单、灵活。

下面针对本方案的细节进行逐一介绍：

Overlay 网络转发流程

报文所属 VXLAN 识别

VTEP 只有识别出接收到的报文所属的 VXLAN,才能对该报文进行正确地处理。

VXLAN 隧道上接收报文的识别：对于从 VXLAN 隧道上接收到的 VXLAN 报文,VTEP 根据报文中携带的 VNI 判断该报文所属的 VXLAN。

本地站点内接收到数据帧的识别：对于从本地站点中接收到的二层数据帧,VTEP 通过以太网服务实例（Service Instance ） 将数据帧映射到对应的 VSI,VSI 内创建的 VXLAN 即为该数据帧所属的 VXLAN。

MAC 地址学习

本地 MAC 地址学习：指本地 VTEP 连接的本地站点内虚拟机 MAC 地址的学习。本地 MAC 地址通过接收到数据帧中的源 MAC 地址动态学习,即 VTEP 接收到本地虚拟机发送的数据帧后,判断该数据帧所属的 VSI,并将数据帧中的源 MAC 地址（本地虚拟机的 MAC 地址） 添加到该 VSI 的 MAC 地址表中,该 MAC 地址对应的出接口为接收到数据帧的接口。

远端 MAC 地址学习：指远端 VTEP 连接的远端站点内虚拟机 MAC 地址的学习。远端 MAC 学习时,VTEP 从 VXLAN 隧道上接收到远端 VTEP 发送的 VXLAN 报文后,根据 VXLAN ID 判断报文所属的 VXLAN,对报文进行解封装,还原二层数据帧,并将数据帧中的源 MAC 地址（远端虚拟机的 MAC 地址）添加到所属 VXLAN 对应 VSI 的 MAC 地址表中,该 MAC 地址对应的出接口为 VXLAN 隧道接口。

Overlay 网关高可靠性

Overlay 网关高可靠性：网关组中网关的 VTEPIP 和 GWVMAC 相同, 均通过路由协议对内网发布 VTEP IP 对应路由；

网关组内部,采用无状态转发设计,所有网关信息同步； 在处理 VSW 发往 GW 的流量时,动态选择 GW 组中的一个 GW,可以很好地起到负载分担的作用； 网关故障后,流量切换到分组内其它网关,保证业务平滑迁移。

网关与内外网设备连接,采用聚合或 ECMP 方式,某 路故障，网关自动切换 路,无需人工干预。单个网关设备采用双主控,原主控故障,新主控接管设备管理,所有处理网关自动完成。转发层面和控制层面分离,SDN Controller 不感知,网关上流量转发不受影响。

控制器集群提供高可靠性

VCF 控制器基于 AKKA 实现了分布式集群管理,AKKA 无中心化的集群成员服务,方便实现无单点故障及无单点瓶颈的大规模控制器集群。

VCF 控制器使用 AKKA Actor 模型构建了一个支持高并发、强容错、大规模应用程序的开放平台。

VCF 控制器集群支持控制器数量的弹性扩展,可以根据网络规模动态伸缩,同时不影响已部署业务,目前最大支持 32 台集群规模，每个控制器集群支持 2.5 万台服务器以及 20 万个虚拟机。

大规模集群设计在提高可靠性的同时,需要在业务的部署上提供完善的架构。传统的一主多备业务模型,只有主节点对外提供服务，其它节点都处于备份状态,主节点会实时把业务数据广播或组播发送给备份节点,完成业务的主备,这种模型在增加集群节点时不能做到业务的 ScaleOut ,相反会影响原有业务规模。每个节点都提供服务、其它节点做为备份的方式,业务模型本质上还是一主多备。VCF 控制器在 AKKA 集群基础上提出了 Region 的概念,很好地解决了上述问题 :

控制器集群提供北向统一 IP ,简化云平台对接 VCF 控制器集群在北向提供统一 IP 地址,北向 APP 无需关心业务所在的集群节点位置,也无需感知集群节点的状态变化,大大简化了编程逻辑。在 VCF 控制器集群中,一部分成员是领导者（leader ），一部分是成员（membe）r 。Leader 对上提供北向的访问接口,负责对集群进行管理； Member 负责管理控制交换机,通过南向接口连接交换机。整个集群可以按需动态或手工形成两台台到多台的子集群,称之为 Region,业务按 Region 运行,也就是说业务的主备以 Region 为单位,在 Region 内完成业务的备份,同时业务也可以在 Region 内以负载均衡的模式运行,以充分利用备份节点的硬件资源。如图所示,我们把所有的 leader 放在一个 Region 里,选一个作为主 Leader,其他的作为备份，这样就保持整个集群有一个持续的不间断的对外提供北向服务的能力。交换机需要同时连到 Region 中的所有成员上，其中一个控制器会被选举为主,其它为备,这样,当 Region 中的主控制器故障时,Region 中的备控制器就可以接管对交换机的控制，提供一个不间断的南向服务能力。

Overlay 网关弹性扩展升级

受制于芯片的限制,单个网关设备支持的租户数量有限,控制器能够动态的将不同租户 的隧道建立在不同的 Overlay 网关上,支持 Overlay 网关的无状态分布,实现租户流量的负载分担。

Overlay 网络可以支持 Overlay 网关随着租户数量增加的扩充,当前最大可以支持超过 64K 个租户数量,从而提供一个具有弹性扩展能力的 Overlay 网络架构,满足 XX 智慧园区大数据云后期弹性扩展的要求。

Overlay 网络虚机迁移

在虚拟化环境中,虚拟机故障、动态资源调度功能、服务器主机故障或计划内停机等都会造成虚拟机迁移动作的发生。虚拟机的迁移,需要保证迁移虚拟机和其他虚拟机直接的业务不能中断,而且虚拟机对应的网络策略也必须同步迁移。

虚拟机迁移及网络策略跟随

网络管理员通过虚拟机管理平台下发虚拟机迁移指令,虚拟机管理平台通知控制器预迁移,控制器标记迁移端口,并向源主机和目 的主机对应的主备控制器分布发送同步消息,通知迁移的 VPort ,增加迁移标记。同步完成后,控制器通知虚拟机管理平台可以进行迁移了。

虚拟机管理平台收到控制器的通知后,开始迁移,创建 VM 分配 IP 等资源并启动 VM。启动后目的主机上报端口添加事件,通知给控制器,控制器判断迁移标记,迁移端口,保存新上报端口和旧端口信息。然后控制器向目的主机下发网络策略。

源 VM 和目的执行内存拷贝,内存拷贝结束后,源 VM 关机,目的 VM 上线。源 VM 关机后,迁移源主机上报端口删除事件,通知给控制器，控制器判断迁移标记,控制器根据信息删除旧端口信息并同时删除迁移前旧端口对应的流表信息。

主控制器完成上述操作后在控制器集群内进行删除端口消息的通知。其他控制器收到删除端口信息后,也删除本控制器的端口信息，同时删除对应端的流表信息。源控制器需要把迁移后新端口通知控制器集群的其他控制器。其他控制器收到迁移后的端口信息,更新端口信息。当控制器重新收到 Packet-in 报文后,重新触发新的流表生成。

Overlay 网络虚机位置无关性

通过使用 MAC-in-UDP 封装技术,VXLAN 为虚拟机提供了位置无关的二层抽象,Underlay 网络和 Overlay 网络解耦合。终端能看到的只是虚拟的二层连接关系,完全意识不到物理网络限制。

更重要的是,这种技术支持跨传统网络边界的虚拟化,由此支持虚拟机可以自由迁移,甚至可以跨越不同地理位置数据中心进行迁移。如此以来,可以支持虚拟机随时随地接入,不受实际所在物理位置的限制。

所以 VXLAN 的位置无关性,不仅使得业务可在任意位置灵活部署，缓解了服务器虚拟化后相关的网络扩展问题； 而且使得虚拟机可以随时随地接入、迁移,是网络资源池化的最佳解决方式,可以有力地支持云业务、大数据、虚拟化的迅猛发展。

Overlay 网络安全部署

如图所示,Overlay 网络的安全部署有三种模式,这三种模式既可以独立部署,也可以配合部署：

主要形态：硬件安全资源。

安全资源旁挂在核心/汇聚设备旁侧（部分安全资源也可选作为 L3 网关） 。

安全资源关注 VXLAN<->VLA 的 N 安全访问控制。

服务器侧部署

主要形态：软件安全资源。

安全资源以 VM 形态部署在服务器内部,可以作为其他 VM 的网关。

如果安全资源支持 VXLAN,可以完成 VXLAN<->VLAN 的安全访问控制。

全硬件 VXLAN 方案不推荐使用。

专用安全区部署

主要形态：软件或硬件安全资源。

安全资源集中部署在某一个 TOR 设备下,重点关注不同 VXLANID 之间互访的安全控制。

如果安全资源支持 VXLAN,就直接配置 VXLAN ID 的互访策略。

如果安全资源不支持 VXLAN ,需要 TOR 完成 VXLAN 到 VLAN 的转换,然后安全资源上配置不同 VLAN 互访的安全策略。

网络技术演进 -vDC 虚拟数据中心

随着虚拟化与云计算技术的不断成熟,XX 市建设允许租户按需租用资源和服务,创建租户自己的虚拟数据中心 （vDC,Virtual DataCenter ） 或虚拟私有云（VPC,Virtual Private Cloud ）,

帮助租户节省建设成本、提高业务敏捷性。因此,XX 市智慧园区大数据云需要考虑后续为各委办局或其他用户提供服务,帮助用户将大部分 IT 应用向智慧园区大数据云迁移。政务专有云平台为租户（委办局单位）提供云主机、云存储、云网络安全等虚拟基础设施资源,基于这些虚拟资源,租户可以在专有云中构建自己的虚拟数据中心,同时各租户的虚拟数据中心彼此安全隔离。

虚拟数据中心（vDC） 的最大好处就是可以让租户灵活部署自己的业务应用,就像部署在自己的专属数据中心内部,拥有计算、存储和网络虚拟实例完整的使用权和管理权。

对于计算、存储资源的虚拟化,目前的技术成熟度很高,使用也非常普遍。然而对于网络安全资源的虚拟化技术实现,是构建虚拟数据中心的重点和难点,XXX 通过多年在网络安全领域的积累,很好的将网络安全的虚拟化技术应用到了 XXXLOU 云 D 平台中,通过硬件设备的 1：N 虚拟化和 NFV（网络功能虚拟化） 技术,实现网络安全资源虚拟化。

由于布线、归属等原因,目前的物理设备并不适合作为租户独享的设备在云计算环境中部署。为了解决目前存在的问题,需要一个既具备物理网络设备的功能又适合于在公有云多租户环境中部署的设备,NFV（Network Function Virtualisation, 网络功能虚拟化） 应用而生。

XXX 提供一系列 NFV 方案,应用于 vDC 场景,帮助 XX 市智慧园区大数据云构建租户的私有云或混合云。它和物理设备一样,采用业界领先的专业网络平台 Comware V7,运行在标准 X86 服务器或虚拟机上,提供和物理设备相同的功能和体验,包括路由、防火墙、VPN、QoS、及配置管理等,同时充分利用虚拟平台的特点,简化设备的部署安装。

13.2.2 安全虚拟化

13.2.2.1 安全网关虚拟化

公有云及私有云等云计算业务的开展,均存在将一台物理设备进行 1：N 虚拟化之后提供给不同租户使用的需求。要求虚拟安全网关之间业务数据相互隔离,能够提供独立管理、独立审计、独立安全策 略，同时能够给每个虚拟安全网关分配独立的处理能力。传统安全网关产品在解决虚拟化问题通常有两种方案：基于虚拟路由或者基于虚拟机。

基于虚拟路由的安全虚拟化方案在数据平面,围绕转发表,通过 VRF 或类似技术将转发相关的表项（如路由表、ARP 表） 分割成多个逻辑的表,实现报文转发的隔离； 在管理平面,为不同虚拟安全网关关联不同的管理员,实现管理的隔离； 在控制平面,需要针对每种业务逐一考虑虚拟化的改造,使其支持虚拟化。这种虚拟化方案,本质上是一种多实例技术,是在已有非虚拟化的系统架构上,对一些主要安全业务进行多实例的改造,只能对个别安全业务实现部分虚拟化， 系统可扩展性差。

基于虚拟机的安全虚拟化方案中 CPU、内存和 I/O 资源由底层的 Hypervisor 或 Emulator 实现模拟。虚拟安全网关作为一个 GuestOS 运行在虚拟化的硬件环境中,因此,基于虚拟机的虚拟化从安全业务的角度来说,是一种完全的虚拟化方案,更容易部署和迁移,也避免了虚拟化后导致的部分功能缺失的问题。但是,基于虚拟机的虚拟化通过 Hypervisor 或 Emulator 作为中间层,给上层构

造了一个完全独立的虚拟硬件空间,每个 GuestOS 需要独立构造完整的操作系统和业务环境,由此也带来了一些问题。比如,单台物理设备/服务器上运行的虚拟安全网关数量很少,报文转发时延加大等。使得这种方案更适合部署在虚拟安全网关数量要求不多、业务性能不高的场景。

虚拟化技术是实现基于多业务业务隔离的重要方式。和传统厂商的虚拟化实现方式不同,XXX 的安全虚拟化是一种基于容器的完全虚拟化技术； 每个安全引擎通过唯一的 OS 内核对系统硬件资源进行管理,每个虚拟安全网关作为一个容器实例运行在同一个内核之上,多台虚拟安全网关相互独立,每个虚拟安全网关实例对外呈现为一个完整的防火墙系统,该虚拟安全网关业务功能完整、管理独立、具备精 细化的资源限制能力,典型示意图如下所示：

1 、虚拟安全网关具备多业务的支持能力

虚拟安全网关有自己独立的运行空间,各个实例之间的运行空间完全隔离,天然具备了虚拟化特性。每个实例运行的防火墙业务系统，包括管理平面、控制平面、数据平面,具备完整的业务功能。因此，从功能的角度看,虚拟化后的系统和非虚拟化的系统功能一致。这也意味着每个虚拟安全网关内部可以使能多种安全业务,诸如路由协议,NAT,状态检测,IPSEC VPN,攻击防范等都可以独立开启。

2、虚拟安全网关安全资源精确定义能力

通过统一的 OS 内核,可以细粒度的控制每个虚拟安全网关容器对的 CPU、内存、存储的硬件资源的利用率,也可以管理每个 VFW 能使用的物理接口、VLAN 等资源,有完善的虚拟化资源管理能力。通过统一的调度接口,每个容器的所能使用的资源支持动态的调整,比如,可以根据业务情况,在不中断 VFW 业务的情况下,在线动态增加某个 VFW 的内存资源。

3、多层次分级分角色的独立管理能力

基于分级的多角色虚拟化管理方法,可以对每个管理设备的用户都会被分配特定的级别和角色,从而确定了该用户能够执行的操作权限。一方面,通过分级管理员的定义,可以将整个安全资源划分为系统级别和虚拟安全网关级别。系统级别的管理员可以对整个防火墙的资源进行全局的配置管理,虚拟安全网关管理员只关注自身的虚拟安全网关配置管理。另一方面,通过定义多角色管理员,诸如在每个虚拟安全网关内部定义管理员、操作员、审计员等不同角色,可以精确定义每个管理员的配置管理权限,满足虚拟安全网关内部多角色分权的管理。

4、接口虚拟化能力

所谓接口的虚拟化,是指物理设备的一个物理接口或者逻辑接口（聚合口或子接口） 同时分配各多个虚拟安全网关,该接口形式上被这些虚拟安全网关共享使用。被共享的接口在每个虚拟安全网关中，分别形成一个独立的逻辑接口实例,可以有虚拟安全网关级管理员各自配置 IP 地址、路由协议、安全业务等。在多个虚拟安全网关实例共享一个 Internet 出口的场景上这种技术可以有效减少对多个物理接口的依赖。防火墙设备只需要通过一个接物理口和外网 Internet 出口路由器相连,通过配置接口虚拟化技术,每个虚拟安全网关实例可以分别分配公网接口,使其具备独立的 Internet 接入能力.

13.2.2.2 虚拟化架构 - 横向及纵向扩展性

传统的虚拟安全网关技术受限于物理设备自身的 CPU 处理能力、内存容量、端口数量等多方面的限制,部署中缺乏扩展性,很难满足业务发展的需求。XXX SOP 虚拟化架构的另一个创新——分布式虚拟 化架构,可以有效提升系统的虚拟化容量。在分布式虚拟化架构中,系统的安全处理引擎可以按需配置,以支持虚拟化能力的线性扩展。虚拟化能力扩展有如下两种方式：横向扩展和纵向扩展。其中横向扩展是指单虚拟墙的处理能力增加,系统整体可支持虚拟墙的总数不变。而纵向扩展则是指单虚拟墙的处理能力不变,系统整体可支持的虚拟墙的总数增加。

同时,SOP 架构可以和 XXX 的 SCF 架构无缝集成,在 N:1 基础上进行 1 :N 虚拟化,实现 N:1 :M。在单台物理防火墙所支持的虚拟安全网关数量、性能不能满足需要时,通过 SCF,进一步扩展虚拟化能力。

13.2.2.3 虚拟化架构 -1 :N:M 虚拟化

在一个虚拟安全网关实例内,虚拟安全网关管理员还可以 续 创建本虚拟安全网关内独立的 VPN 多实例 (VRF),不同虚拟墙内的 VRF 实例完全独立,名字可以相同。同一个虚拟墙内多个 VRF 共享该虚拟安全网关的资源,通过抢占进行分配。通过这种 1 :N:M 虚拟化方式可以满足一个租户内部的进一步业务隔离需求,同时进一步扩大系统虚拟化能力。上述功能尤其适用于部分变更频繁且有实时性要求的业务系统,可以开通独立的虚拟安全网关并且将该虚拟安全网关授权给业务系统管理员,并且限定业务系统管理员的权限,比如仅能操作该虚拟安全网关内的安全安全策略。对于其他的业务系统,可以在缺省虚拟安全网关内通过 VRF 隔离,由管理员统一维护管理。此方案实现了业务快速响应、虚拟化业务能力扩展及安全权限控制的多方平衡。

13.2.2.4 虚拟化架构 - 接口共享虚拟化

共享 Internet 出口场景

如果多部门共享 NAT 出口或者是 VPC 应用场景中对外的 internet 互联 路只有一条,那么对应的对外物理互联接口就只有一个。待解决的问题就是如何实现多虚拟安全网关共享该物理接口。划分子接口并将不同的子接口分配给不同虚墙的方式不可行,因为 internet 返回的流量不会携带任何 VLAN TAG。传统的解决方案可以前置出口路由器,通过出口路由器上配置复杂的 NAT 转换策略,并通过多个子接口和防火墙互联以区分虚拟安全网关数据,但是这种方式存在配置复杂,增删虚拟安全网关需要同步修改上层路由器配置的问题,管理维护都很麻烦。

针对该应用场景,XXX SOP 架构创新性地推出接口共享虚拟化特性。物理设备的一个接口 (可以是物理接口也可以是逻辑接口) 同时分配给多个虚拟安全网关,该接口形式上被这些虚拟安全网

关共享使用。这种方式中,被共享的接口在每个虚拟安全网关中,分别形成一个独立的逻辑接口实例,可以由虚拟安全网关级管理员各自配置 IP 地址、路由协议、安全业务等。该接口在不同的虚拟安全网关实例中会自动生成不同的 MAC 地址 (虚拟安全网关管理员也可以手工修改 MAC,) 系统根据数据报文携带的 MAC 地址可以区分所属的虚拟安全网关。

13.2.2.5 虚拟化架构 -N:1 虚拟化

现有的双机热备技术难以满足云计算时代的规模管理部署、性能弹性扩展需求。云时代迫切需要一种全新的架构,能够在满足热备可靠性的基础上解决现有缺陷。

安全集群框架(SCF) 高可靠性技术通过将两台设备虚拟化为一台逻辑设备,实现了管理和控制上的统一,同时组网部署更加简单,有效利用 路带宽,提高系统稳定性,大幅减少故障点带来的业务切换冲击。

SCF 技术脱胎于 XXX IRF2 技术,将 IRF 从网络层面上升到业务层面,承了 XXX IRF2 网络部署的种种优点,实现了安全业务的集群处理。目前 SCF 最多支持 4 台分布式设备的集群,极大地方便了用户的灵活扩容。SCF 在拓扑管理、成员管理、堆叠分裂检测等方面的实现机制与 IRF2 相同,本文不再赘述。本文重点以分布式设备来说明安全业务的备份机制。

在 SCF 集群中,包含如下几个关键概念:

安全引擎组:由多个安全引擎组成的逻辑实体,通过安全引擎组实现了安全引擎的资源池化。业务配置、虚拟设备划分都是以安全引擎组为基础。

智能引流策略:为了实现系统性能的线性扩展,需要能够将数据流负载分担到安全引擎组内的多个安全引擎。同时由于安全业务的有状态行,需要通过引流策略保证同一条数据的往返报文由同一块安全引擎处理。由于这些引流策略是由系统自动生成,称之为智能引流策略。

备份组:备份组是一个逻辑概念,一个组内最多包含两个引擎,同一个引擎可以属于不同的备份组。同一备份组内两个引擎根据优先级决定主备关系。智能引流策略根据备份组内引擎的主备关系将数据流引流到主引擎上。

1 、引擎级备份支持更高可靠性

为解决传统双机备份“故障出发点多” 及“切换粒度 ” 带来的业务冲击及性能损失问题,SCF 架构引入了引擎级备份技术。引擎级备份通技术过将主机进行 SCF 集群,对外通过跨设备 路捆绑或者提供等价路由节点进行互联,有效利用 路带宽。对内在业务引擎之间实现备份,从而将主控、接口和业务引擎的故障解耦,可以最大程度地减少各节点故障带来的业务冲击。

在一个 SCF 内的多个安全业务引擎,通过配置指定 1 :1 的备份关系。从可靠性角度考虑通常建议备份组内的两个成员引擎位于不同的机框,避免整机掉电带来的业务中断。在偶数块引擎的情况下,可以实现引擎 1 对 1 的备份。在奇数块引擎的情况下,可以采用循环备份法比如,1、2、3 三个引擎,2 备份 1 ,3 备份 2,1 备份 3。系统根据配置的引擎备份关系进行引流,同时实时监控业务引擎的运行状态。

一旦发现引擎故障,那么将该引擎承载的数据流切换到备份引擎上。

具体备份切换原理如下图所示：FW1-2 作为 FW1-1 的备份引擎,FW2-1 作为 FW1-3 的备份引擎,FW2-3 作为 FW2-2 的备份引擎。正常情况下，系统引流到引擎 FW1-1、FW1-3、FW2-2 上,当任意一块主引擎故障时，该主引擎承载的数据流被分发到其对应的备份引擎。

在引擎级备份情况下,当一块引擎发生故障时,仅仅在该引擎所在的备份组内切换,在此过程中外部节点无感知,路由无收敛。主控切换外部无感知,路由无收敛。而接口故障通过 路聚合可以快速收敛。并且任一组件的故障切换不会导致其他组件的切换。通过这种机制实现故障 0 中断或毫秒级切换。同时,任意一块业务引擎故障,仅仅影响该业务引擎上承载的业务,其他业务引擎承载的业务不受影响,一方面最大程度地避免了切换对于切换的冲击,另外一方面也保留了系统的最大性能（仅损失一块引擎的性能） 。

2 主机级备份支持灵活组网

引擎级备份技术对外体现为虚拟化的安全资源池,非常适合云计算环境下的部署,也具备很高的可靠性优势。但是目前很多传统网络中网络设备的部署还是采用传统的主备冗余方式比如 VRRP 。在这种场景下,安全设备需要支持主备模式与上下游的网络设备互联。在 SCF 架构中这种技术称之为主机级备份。主机级备份的几个主要概念如下：

节点 (Node):一个 Node 代表一台设备,Node 的主备状态由 Node 的优先级确定。Node 主备状态可以理解为业务数据层面的主备,该主备状态与 SCF 管理控制层面上的主备相互独立,二者主备状态可以不一致。同时 Node 的主备状态也决定本框接口和引擎活动状态及路由的发布的优先级。Node 节点监控本 Node 所在设备的接口状态、引擎状态并指定每一个监控对象对应的权值。任意监控对象故障,Node 会把初始优先级减少该监控对象对应的权值,如果该 Node 的优先级小于等于 0，并且另一个 Node 优先级大于 0,那么 Node 之间进行主备切换。

在实际部署中,通常建议配置为任意一个监控对象故障都发生切换。

冗余口：冗余口是一种全局逻辑接口,每个冗余口允许加入最多两个其他类型的成员接口,通常是每个 SCF 成员各出一个本框接口作为成员口。成员口类型可以为普通以太物理口、聚合口和子接口。成员接口在加入冗余口时,根据 Node 的优先级确定该接口的 active/inactive 状态,处于 inactive 状态的接口丢弃所有接收到的报文。IP 地址、业务等都是在冗余口下配置。

备份组（Failover Group ）：备份组的概念参考上文说明。

冗余组：一个冗余组定义了一条转发 路上的主备关系。冗余组的成员包括 Node、备份组和冗余口,通过 Node 的主备关系，同步切换冗余组内的多个冗余口及备份组成员的 active/inactive 状态,从而保证上下行的切换联动一致。

在主机级备份技术中,流量同一时刻只会在一个机框内转发,会话的备份只能在主机框的引擎和备机框的引擎之间做 1 对 1 的备份。

机框 1 和机框 2 组成高可靠性,机框 1 为 Node1,机框 2 为 Node2。Node1 优先级高,所以机框 1 为 Active 。机框 1 的 3 块引擎和机框 2 同槽位的 3 块引擎组成 3 个备份组。同时机框 1 的出入接口分别和机框 2 的出入接口组成出入冗余口。当备份组和冗余口加入冗余组时，备份组成

员和冗余口成员的优先级统一由 Node 的优先级来控制。这样可以保证流量只上机框 1,并且仅被机框 1 引 擎处理。当机框 1 上的入口、出口或任意引擎故障,触发冗余组切换到机框 2,同时机框 2 的引擎和接口切换为 Active ,后续流量从机框 2 进行转发。

3、scale-out 弹性扩展多框集群

单台物理设备受限于自身 CPU 处理能力、内存容量、硬件槽位等多方面因素,整体处理能力存在上限。传统 IT 部署模式下,为了满足未来三到五年的业务流量需求,通常会购买远超实际需求的高端设备，导致资源利用率低下和投资浪费。SCF 架构基于 Scale-out 弹性扩展方式实现多台机框（最多 4 台） 的集群,实现系统性能的弹性增长。同时支持异构集群,可以将两台不同性能的设备进行集群,便于用户按需采购和部署,保护投资。多框集群的另外一个应用场景就是双活数据中心,通过跨数据中心部署多设备集群,并且在跨数据中心的两台设备之间开启会话备份,实现业务故障、业务迁移、数据中心故障等多种场景下可靠性。

13.2.2.6 安全功能虚拟化 - 虚拟软件安全网关

数据中心中虚机 （VM） 间的交互流量,我们称之为“东西向流量” 。针对东西两流量,本项目采用虚拟软件安全网关（XXX VFW1 OO）0 产品来实现安全防护。

对于普通的云计算 VPC 模型的业务,既可以将 NFV 安全业务安装在业务服务器内,也可以部署独立的安全业务网关服务器。在本次项目中,我们采用部署独立的安全业务网关服务器,此时安装了 NFV 的独立的服务器资源逻辑上被认为是单一管理节点,对外提供高性能的 VFW 业务。

考虑到在虚拟化之后服务器内部的多个 VM之间可能存在流量交换,在这种情况下外部的安全资源池无法对其流量进行必要的安全检查,在这种情况下,XXX 推出了基于 SDN 架构模式的虚拟化软件安全网关。XXX NFV 产品 VFW1000 基于专业的 XXX Comware V7 平台,在安全功能方面,为用户提供了全面的安全防范体系和远程安全接入能力，支持攻击检测和防御、NAT、ALG、ACL、安全域策略,能够有效的保证网络的安全； 采用 ASPF（Application Specific PacketFilter ）应用状态检测技术,可对连接状态过程和异常命令进行检测，提供多种智能分析和管理手段,支持多种日志,提供网络管理监控，协助网络管理员完成网络的安全管理； 支持多种 VPN 业务,如 L2TPVPN、GRE VPN 、IPSec VPN 等丰富业务功能。

XXX VFW1 OOO 带来如下优势：

部署简单,无需改变网络即可对虚拟机提供保护

安全策略自动跟随虚拟机迁移,确保虚拟机安全性

新增虚拟机能够自动接受已有安全策略的保护

细粒度的安全策略确保虚拟机避免内外部安全威胁；

XXX VFW 解决方案能够监控和保护虚拟环境的安全,以避免虚拟化环境与外部网络遭受内外部威胁的侵害,从而为虚拟化数据中心和云计算网络带来全面的安全防护,帮助用户构建完善的数据中心和云计算网络安全解决方案。

在部署软件安全网关进行内部 VM 之间流量安全检查的过程中，涉及到以下几个方面的步骤：

A） 软件定义流量策略：首先将需要进行安全防护的 VM 之间的流量进行精确定义,用户可以通过 IP 地址/MAC 地址或者是基于 VM 的名字进行策略定义,并进行允许或拒绝等动作的配置。

B） 软件决定转发：虚拟交换机在接收到 VM 的流量后,自动该该流量首包上送到 SDNController ,之后根据预先配置的安全策略，形成 OPENFLO 的 W 流表下发到本地虚拟交换机。后续报文经过虚拟交换机时将检查转发表项,对符合规则的报文转发到软件安全处理引擎。

C） 软件实现安全：初始化过程中,管理中心将负责对虚拟机安全软件完成必要的安装和初始化配置,并为该虚拟机分配合理的硬件资源并对该安全业务能力进行设定,同时根据业务的需求下发各种安全策略。在流量到达本虚拟机时,该软件安全网关将完成各项安全检查。完成安全检查的用户流量将自动转发到目地 VM 虚拟机。

D） 软件实现业务编排：对于部分业务需要进行多安全业务处理时，可以在服务器内部配置多个安全业务处理引擎,此时可以通过管理层对这部分流量的转发路径进行定义,并生成具体的路由配置策略、或者是通过 VPN 隧道等方式,实现对报文在多业务之间的路径选择的智能化以及报文封装转发的自动化。

13.2.2.7 安全虚拟化与安全服务

传统安全业务的部署,通常基于物理拓扑,将安全设备串行到业务流量路径当中,这种部署模式存在如下问题:业务上线或业务变更需要调整整个路径下设备的策略,无法满足快速变更的需求； 设备能力扩展性较差,一旦出现性能不足,通常只能更换更高端的设备； 设备的能力无法在多业务间共享； 传统基于路径的部署方式无法应用于 Overlay 网络。

新 IT 架构下,安全部署模式需要随之发生变化,基于 Overlay 网络构建集中的安全能力资源池。通过集中的控制器将需要进行安全防护的业务流量引流到安全能力中心进行防护,并且根据业务需求编排安全业务的防护顺序,也就是通常所说的服务 。由于实现了物理拓扑的解耦,所以能够很好地支持安全能力的弹性扩展及多业务能力共享。

1 、安全服务 概念

数据报文在网络中传递时,根据业务类型、安全保护的等级要求需要经过各种各样的安全服务节点,这些安全服务节点包括熟知的防火墙、入侵检测、负载均衡等。通常,网络流量需要按照业务逻辑所要求的既定顺序,穿过这些安全服务节点,这就是所谓的服务（Service Chain ）,可见,服务 并不是一个新的概念。

随着 SDN 及网络虚拟化的不断推进,服务 逐渐变得更加重要。

在 Overlay 网络下,服务 的各服务节点可能位于相同或者不同的安全能力资源池。通过面向租户、面向应用的服务 编排界面,自动下发引流策略,进行相应的安全防护,从而达到或优于传统安全防护的效果。

2 、服务 的封装格式

NSH(Network Service Header) 是专门为服务 而设计的一种扩展头格式,可承载于 VXLAN 、GRE 等多种 Overlay 封装中,其格式如下：

NSH 中因为有 protocol 字段,因此可以承载二层用户报文、三层用户报文,较为灵活。扩展性强,可以支持携带多个业务上下文信息。但是由于较为复杂,所以硬件芯片支持较为困难。

与之对比一种更为简单的封装方式则是使用 VXLAN 头中保留字段的方式,其格式如下 ：

扩充 8 字节的 VXLAN 头,从保留字段中抽出 24 字节做 ServicePath ID ,通过 Service Path ID 唯一地确定一个业务 ,虽然无法携带更多的业务信息,但是由于封装简单,所以硬件芯片支持非常容易。xxx 的服务 缺省使用这种格式进行封装。

3、服务 模型中的主角

在服务 模型中,涉及到服务 定义、引流下发、服务 报文封装、服务 业务处理等多个环节,各功能节点对应的业务组件如下。

控制平面（Control Plane ）

管理服务 域内的设备,创建服务 ,将服务 的配置信息,下发到各个相关节点上,目前主要是通过 Controller 实现,对用户的业务界面主要由 IMC CSM 组件实现。

流分类节点（Classification ）

匹配流分类规则的数据报文,会按照要求被转发到服务 中处理。最初的流分类节点,部署在服务域的边缘,即所谓的服务 接入点。服务 之间,也可以依靠流分类衔接。如图 4 所示,xxx 服务模型接入点包括如下四种类型 :支持业务 的 Vswitch ：由 Vswitch 接入 VM 报文后直接做流分类,增加业务 Overlay 封装。

交换机接入普通 Vswitch ： VM 通过普通 Vswitch 接入,Vswitch 仅作二层交换使用,上送 VXLAN GW 设备后,由 VXLAN GW 设备进行流分类,增加业务 Overlay 封装。

交换机接入物理设备：交换机直接接入物理服务器,对物理服务器发送的用户报文做流分类后,增加业务 Overlay 封装。

交换机接入普通 VXLAN ：Vswitch 作为 VXLAN 的 VTEP,将普通 VXLAN 报文上送到 VXLAN G，W 由 VXLAN GW 设备进行流分类，换成业务 Overlay 封装。

服务节点（Service Function ）

服务节点作为资源被分配使用,它的物理位置可以是任意的,分散的,通过服务 的串联,完成预定义的工作。如图 5 所示,xxx 服务 模型中服务节点包括如下两种类型。

支持服务 功能处理的节点：包括 xxx 新一代硬件安全设备或虚拟的软件安全设备,能够识别服务 封装报文,并对业务内部封装报文进行安全处理,处理完毕后修改 VXLAN 封装并转发到下一个安全服务处理节点。

不支持服务 功能处理的节点：包括 xxx 传统安全设备或者第三方安全设备。这些服务节点不支持识别服务 封装报文,必须通过代理节点（通常为接入交换机） 将服务 头剥掉后转发给服务节点,服务节点处理完毕后再转发给代理节点,代理节点转发给下一个服务节点或目的 VM。

代理节点（Proxy Node)：对于不支持服务 封装的业务节点,需要通过代理节点剥离服务 封装,

将业务策略信息转换成 VLAN 等，转交给服务节点处理。

4、服务 处理流程

如上文所述,在服务 模型中,控制器会给服务 接入点下发引流策略及服务 信息（Service Path ID 和第一个安全服务节点 IP ），服务 节点匹配引流策略,然后对数据流进行服务 VXLAN 封装,然后通过 Overlay 网络转发到第一个安全业务服务节点。支持和不支持服务 报文识别的两种节点的处理机制稍有不同下文分别说明一下：

支持服务 报文处理的服务节点

对于支持服务 报文处理的服务节点来说,在服务 配置过程中,控制器会给服务 中的每一个节点下发对应业务 ID 的上一个服务节点 IP(Pre-Node IP ）和下一个服务节点 IP（Next-Node IP ），对于第一个节点只有 Pre-Node IP ,而对于最后一个节点则只有 Next-Node IP,同时会下发前后 Node IP 对应的 Fib 表项。当服务节点收到一个 VXLAN 报文时,会根据 VXLAN 报文中携带的 Service PathID 查找相应的业务 表项,如果匹配上则进行解封装,针对解封装后的报文进行安全业务处理,做完安全业务处理后,查找服务 对应的 Next-Node IP ,并进行服务 封装,转发到下一个服务节点。如果本安全节点就是最后一个服务节点,那么在进行完安全处理后,要根据内层载荷的目的 IP 做普通的 VXLAN 转发,也就是根据目的 VTEPIP 进行 VXLAN 封装。支持 VXLAN 报文识别的服务节点模式对基础网络设备无特别要求,兼容性较好。

不支持服务 报文处理的服务节点

在服务 部署模型中,通过代理节点方式兼容传统的安全设备或者第三方设备。以下图 6 为例说明：控制器给服务 接入点下发的 IP 为代理节点 IP ,同时控制器会给代理节点下发服务 处理信息。

当代理节点收到服务 报文时,首先匹配北向南服务 信息,然后将报文转发到 FW 服务节点,FW 服务节点处理完毕,通过 Inline 转发返回给代理节点,代理节点 续匹配南向北服务 信息,然后将报文转发给 IPS 服务节点,IPS 服务节点处理完毕,通过 Inline 转发返回给代理节点,代理节点在匹配不到服务 信息的情况下走 VXLAN 正常转发,将报文转到目的 VTEP1。在这种模式下安全服务节点可以单臂模式部署,也可以双臂模式部署。

这种部署模式,对安全设备要求较低,但是对代理节点要求较高， 需要支持大容量 ACL 表项,在实际部署中存在一定局限性。

5、安全服务 典型部署模式

数据中心通常存在两类流量：东西流量和南北流量。所谓南北流量是指从服务器到 Internet 网络的纵向流量,而东西流量则为服务器之间的横向流量。安全服务 需要对这两种流量进行防护。

南北流量防护模式

南北流量的防护模式分为以下两种。模式一采用一体化的 NGFW 设备实现 VXLANIP GW 及多业务安全防护的功能,部署模式上符合服务 模型,实现了安全设备与物理拓扑的解耦。安全功能执行与传统设备无差异。优点是支持全业务安全功能,但存在无法按需调整安全功能处理顺序问题。模式二通过采用不同的安全设备实现不同的安全功能,实现了功能级别的安全资源池,是真正意义上的安全服务 模型,可以满足灵活的业务防护需求。

在这种部署模式中,NGFW 设备作为 VXLAN IP Gateway 终结租户的 VXLAN 流量,并转换为 VLAN 流量转发到 Internet ,反向实现 VLAN 到 VXLAN 的转换。NGFW 同时支持 NAT、安全域、IPS、SLB 等多种功能。通过创建不同的虚拟防火墙对应不同的租户。VXLAN 网关可以部署多台,通过控制器下发的引流策略实现多台 VXLAN 网关的负载分担。这种模式部署简单,在控制器上仅管理一种设备类型。如果要实现差异化的服务,通过在设备增加或删除配置即可。这种部署模式的缺点就是同一台设备上集成了多业务的功能,多业务之间的处理顺序由设备本身的业务实现逻辑决定,无法调整。

南北流量防护模式

在这种部署模式中,将 LB 功能和 IPS 功能分离出来采用单独的设备实现,在最外层采用防火墙设备作为 VXLAN 网关实现 VXLAN 和 VLAN 之间的互通。由于采用单独的 IPS 和 LB 设备,控制器根据租户需求进行业务编排可以控制流量只经过 FW 和 LB 或者是只经过 FW 和 IPS。采用这种部署好处就是业务处理节点清晰,并且不同节点仅实现相对单一的功能,可以做到更高的性能。

东西流量防护模式

东西向流量通常是租户内部的流量比如 WEB 到 APP 服务器,或者是 APP 服务器到 DB 服务器。租户内部流量通过 Overlay 网络转发，所有的安全业务节点处理的都是 VXLAN 的报文。通过控制器编排下发的引流策略按需按序穿过各安全业务节点。

6. 安全服务 的价值

新 IT 架构下,基于 Overlay 网络,建立统一的安全能力资源池，实现安全能力部署与物理拓扑的解耦,从而支持安全能力的弹性扩展及资源共享,支撑 IT 业务的快速上线及变更。同时,基于安全服务技术,IT 管理员可以基于风险评估结果实时动态调整安全策略，增加新的安全防护能力,实现整网主动安全防护。

13.2.2.8 采用服务方式的安全控制

在 XX 市智慧园区大数据云数据中心中,虚机间的流量访问控制及威胁检测依赖 NFV 资源池。

NFV 资源池中的 VFW 支持透明模式部署,满足内部 VM 间安全防护需求； 支持透明模式部署,提供对数据中心内 VM 间流量防护：

1 ）设置安全策略控制对 VM 虚拟机之间的访问,对这些 VM 之间的流量访问进行允许或禁止；

2） 对 VM 之间的流量互访进行攻击检测,及时发现内部攻击行为。

虚机间的流量要想按需调度到NFV资源池中,要依赖于SDN+VXLA技N术,还要依赖服务 技术。数据报文在网络中传递时， 需要经过各种各样的业务节点,才能保证网络能够按照设计要求,提供给用户安全、快速、稳定的网络服务。网络流量按照业务逻辑所要求的既定的顺序,经过这些业务点,这就是服务 。

传统网络中的防火墙、负载均衡器等业务节点和网络拓扑有 密的耦合,部署较为复杂,在服务变更、扩容时,都需要改动网络拓扑,并重新进行网络设备的配置。随着 NFV 技术的的发展,业务节点可以方便的部署在虚拟化网络甚至直接安装到服务器中。为了引导网络中的业务报文次序通过虚

拟化网络中的多个业务节点处理后再进行转发,需要 SDN 的服务 功能来实现。服务 是支撑虚拟化、业务网络可编程的关键技术。

简单来说,本项目中采用的 VFW1 000 实际是作为一个特殊的虚拟机运行在虚拟平台中,正常情况下 VM 间访问流量直接经过 vSwitch 互访,当需要对其进行安全防护时,管理员配置通过 SDN 控制器创建服务 策略,当 VM 间第一次发生交互流量时,vSwitch 会向控制器申请的引流策略（包含服务策略的流表） ,策略下发后,vSwitch 根据流表内容对流量进行匹配,将需要防护的流量引流到 VFW 中,由 VFW 对虚拟机间流量进行防护处理,最后经 VFW 处理过的流量再回到 vSwtich 中进行正常转发.

13.2.3 计算虚拟化

部署虚拟化管理平台,用作实现对硬件资源的虚拟化,以及对虚拟资源、业务资源、用户资源的集中管理。此外,为上层云平台提供统一的接口,用于支持上层不同的业务调度与应用部署。要求虚拟化平台能够至少支持以下要求:

13.2.3.1 虚拟化资源池

本项目主要用于市级平台业务专网与公众服务网,首先需要保证本系统的安全,所以选用的虚拟化软件必须是国内成熟稳定的虚拟化软件,实现各子系统的计算资源和存储资源的动态伸缩和分配管理，便于按上层业务应用系统需求灵活分配资源。规划部署计算资源池时,要参考安全等级保护要求,使整个虚拟化系统需具有以下特点:

通过虚拟机 HA、虚机热迁移、存储热迁移功能,能够有效减少设备故障时间,确保核心业务的连续性,避免传统 IT ,单点故障导致的业务不可用。

易实现物理设备、虚拟设备、应用系统的集中监控、管理维护自动化与动态化。

便于业务的快速发放 , 缩短业务上线周期,高度灵活性与平滑可扩展性,提高管理维护效率。

利用云计算虚拟化技术可自动化并简化资源调配,实现分布式动态资源优化,智能地根据应用负载进行资源的弹性伸缩,从而大大提升系统的运作效率,使 IT 资源与业务优先事务能够更好地协调。

13.2.3.2 虚拟化安全隔离

为了满足各个平台之间的相互独立,互相不影响。通过虚拟化隔离、VLAN/VxLan 网络划分、安全组隔离手段保障计算、存储、管理、接入等域的安全隔离。按照等级保护不同级别划分逻辑隔离的主机资源池,对应相同级别的业务系统可通过虚拟机部署于同一级别资源池,业务虚拟机仅能在相同级别主机池内迁移。虚拟化平台提供包括 CPU 调度、内存、内部网络隔离和磁盘 I/O 、虚机存储的安全隔离。

13.2.3.3 虚拟机/ 存储热迁移

提供基于共享存储的迁移以便满足数据中心虚拟化项目的业务连续性要求。虚拟机热迁移特性是指在使用同一共享存储的主机之间将处于运行态的虚拟机由当前所在的主机迁移到另一台主机上,在迁移的过程中不影响用户对虚拟机的使用。

在对主机进行维护操作前将该主机上的虚拟机迁移到其他主机上,然后再作维护,可以降低因主机维护造成的用户业务中断。

通过将繁忙的主机上的虚拟机迁移到空闲的主机上,可以提升虚拟机用户的感受,并使全局业务均衡。

通过将空闲主机上的虚拟机聚拢到几台主机上,然后将没有负载的主机关闭,可以降低数据中心的电能消耗。

在虚拟机正常运行时,通过管理员手动操作,将虚拟机的卷迁移至其他存储单元中,可以在虚拟化平台下的同一个存储设备内、或不同存储设备间进行在线迁移。存储迁移带宽可控,避免对正常业务产生影响,支持跨集群迁移。存储热迁移技术便于对现有存储系统的扩容,减容,便于存储系统的更新换代。

13.2.3.4 虚拟机高可靠 HA

虚拟化平台提供故障自动迁移（虚拟机 HA(High Available) ）机制,可提升虚拟机的可用度,允许虚拟机出现故障后能够重新在资源池中自动启动虚拟机。

系统周期检测虚拟机状态,当物理服务器宕机、系统软件故障等引起虚拟机故障时,系统可以将虚拟机迁移到其他物理服务器重新启动，保证虚拟机能够快速恢复。目前系统能够检测到的引起虚拟机故障的原因包括物理硬件故障、系统软件故障。

13.2.3.5 虚拟机规格动态调整

虚拟机根据应用系统的性能需求,虚拟化平台可以灵活调整虚拟机的配置规格,包括调整 vCPU 个数,内存大小,网卡个数、磁盘卷个数,调整虚拟卷的大小,纵向扩展有效保证单个虚拟机 QoS。虚拟机快照备份技术。

虚拟化平台自带虚拟机快照备份系统,不需要与第三方的备份软件结合,也不需要额外费用,备份系统就可以对虚机卷（包括系统卷和/ 或数据卷） 数据进行备份。备份过程不需要终端用户参与,也不需要在 VM 里安装代理,且不影响生产系统的运行。当生产系统由于意外丢失 VM 卷数据时,系统管理员可以通过本地备份系统恢复 VM 卷数据,以保证 VM 能 续正常工作。

管理员接入备份管理系统可以进行选择虚拟机、或虚拟机的某个卷进行备份,灵活设置备份策略,备份起始时间、配置全量备份和增量备份的周期。管理员可以根据备份文件恢复虚机,可以从存储读

取快照文件恢复虚拟机。管理员可以选择恢复到原有虚机、或者新虚机、或者其它虚机。

13.2.3.6 自动化弹性调度

为了便于后续数据中心的人员运维,虚拟化平台需要提供丰富的自动化运维技术。虚拟化平台提供资源弹性统一调度,支持设置集群资源的调度策略,根据管理员设置的调度策略,可根据应用系统的负载进行自动化调度运维,大大地减少了运维人员的工作量。根据应用场景,提供三种策略类型:弹性资源扩展策略、动态资源调度策略、动态电源管理策略。

（1） 弹性资源扩展策略

针对单独的应用而言,应用根据应用的当前负载动态的调整应用实际使用的资源,当一个应用资源负载较高时,自动添加虚拟机并且安装应用软件； 当应用的资源负载很低时,自动释放相应的资源。

（2） 动态资源调度

当单一宿主服务器不足的情况下,系统可以根据策略调整本物理主机虚拟机承载数量,通过自动化动态迁移的方式调度部分虚机到较空闲的物理主机上,保证主机池所有物理服务器都工作在比较健康的状态。

（3） 动态电源管理策略

时间计划策略允许用户对于不同的应用实现资源的分时复用。用户可以设置计划策略,使得不同的应用分时段的使用系统资源,比如说白天让办公用户的虚拟机使用系统资源,到了晚间可以让一些公共的虚拟机占用资源。

虚拟化平台提供多种自动化调试策略,包括节能策略、负载均衡策略。便于用户合理利用资源。可以实现节能降耗,实现轻载合并下电,重载分离上电。

系统负荷不大时,各 VM 占用 CPU 较低,部分 VM 关机了,可以将某些服务器上的虚拟机自动迁移到其他节点,对这个服务器进行休眠或下电,实施系统节能策略。

系统重载时,再让部分物理机上电,并迁移 VM 到新物理机,保证用户感受。系统需分析并选择合适的物理机上下电,减小迁移的 VM 数目。

13.2.4 存储虚拟化

依据 XX 市政府当前业务应用系统对资源需求以及业务重要性的不同,在 XX 市智慧园区大数据云中提供高性能型和容量型两类存储资源池。

高性能存储资源池：采用基于 FC SAN 或者 IP SAN 架构的高端集中式存储系统来提供存储资源,用于支撑政府关键业务系统和对磁盘性能要求高的业务应用系统。

容量型存储资源池：采用分布式存储系统,为非关键业务系统和对磁盘性能要求较低的业务应用系统提出存储资源。

13.2.4.1 集中式存储规划设计

卓越的、 大规模的， 自动负载均衡的存储系统高可用高性能 - 卓越的 ASIC 芯片提供如下特性：

零感知

快速的 RAID5 RAID6 迅捷的磁盘恢复技术

精密相连的集群高带宽， 低延迟， 高速互联

混合任务并发处理数据和控制信息的独立分类处理

优势介绍

1） 提高业务灵活性

a）高性能、 可大规模扩展、 动态分层的 P8*** 阵列是 xxx 融合基础设施的一部分， 可帮助客户控制 IT 无序增长造成的僵化问题和高昂成本，以便可以将资源从运营转移到创新和战略计划上。

b）快速、 自动配置能力能够支持客户减少新项目的部署窗口， 并加快新应用和服务的上市速度。

c）可选的 P8*** 动态优化和自适应优化软件具备自动服务级别优化能力， 可以灵活地迅速响应不断变化的应用和基础设施要求， 而无需进行主动管理。

d）P8*** 精简配置软件能够支持瞬捷部署新应用和配置新客户端， 无需依赖传统的存储采购周期。

e）安全多租户支持使用 P8*** 虚拟域技术（ 市场上首款也是唯一一种类似于存储管理程序的技术 ）实现定制、 改进的安全特性，甚至能够为多个内部或外部客户提供安全可靠的 “自助” 存储。

2） 降低存储总体拥有成本多至 50%

a）高级的内部虚拟化、 宽条带化和混合工作负载支持可降低物理容量的采购、 存储开销、 功耗和散热需求， 而丝毫不会影响性能。

b）位于每个控制器节点内的两个 Gen4 ASIC 含有 Thin Built In 功能， 可以实现基于硬件的精简转换以降低传统的存储容量要求并且回收已分配但未使用的容量， 从而保持最佳容量利用率。

c）通过支持客户可以只购买实际需要的磁盘容量（ 只在实际需要写入数据时 ）， 精简配置软件可显著减少容量浪费情况。

d）与虚拟复制软件（ 一款无预留、 写时复制的精简技术 ）配合使用， 可降低频繁的磁盘快照产生的容量， 并且可以创建能够立即安装并使用的数据副本。

e）快速 RAID 5 可将 RAID 5 的性能提升至接近 RAID 1 的水平， 并大幅降低容量开销； 快速 RAID 6(RAID MP)可实现增强的保护，同时性能仅略低于 RAID5， 使客户全面采用更高可靠性的 RAID6 技术成为可能。

3） 将管理效率提高多至 1 0倍， 帮助实现云计算

a）运行在所有阵列上的 InForm 操作系统软件提供了大幅简化的自动配置和管理能力， 能够帮助管理员减轻繁琐的手动管理任务， 并降低发生错误的可能性。

b）精简配置软件消除了阵列规划工作，让管理员在应用生命周期中只需对存储进行一次配置。

c）简单、 统一的管理控制台和极其强大且可编写脚本的命令行界面(CLI) 提供了行业领先的易用性， 包括能够在几分钟内完成多模式、 多站点灾难恢复配置。

d）UIS 集成为公共和私有云环境的存储配置及扩展提供了一种简化的途径。

e）动态优化和自适应优化软件可支持 P8*** 系统自动、 智能地满足服务级别的变化， 无需进行主动管理。

价值场景展现

1） 典型问题： raid 受限于物理磁盘数量

在传统阵列存储系统中， 创建 raid 是基于从盘的数量， 但是为了 保证 raid 的性能， 一个 raid 组的磁盘数量是有限的， 例如一个 raid5 或者 raid6 ， 磁盘数量一般不会超高 1 2 个（在厂家最有配置设计中） ， 而 raid 的性能也就仅限于这些磁盘的性能。

2） 解决之道： 不再依据物理磁盘创建 raid

xxx 存储系统中创建 raid 不是基于物理磁盘， 而是基于每个物理磁盘上的存储块。 在配置存储时， 现将存储系统中的所有磁盘空间按照一定大小容量的块将所有磁盘打散， 在依据不同磁盘上这些块创建 raid 。 这样就会使得一个 raid 最大可以发挥整列上所有磁盘的性能。

13.2.4.2 分布式存储规划设计

ONEStor 存储方案采用分布式存储技术， ONEStor 架构的基本单元是 x86 标准服务器， 用户无需像以往那样购买连接计算服务器和存储设备的 SAN 网络设备（ FC SAN 或者 iSCSI SAN)。 在同等存储容量下， 不采用特殊专用硬件， 存储性价比比传统存储产品有显著提升。

ONEStor 拥有灵活的部署方案， 根据实际的硬件性能、 应用场景，可以将计算虚拟化与存储虚拟化进行分离部署或融合部署。

技术特点

XXX ONEStor 存储系统采用分布式设计， 可以运行在通用 x86 服务器上， 在部署该软件时，会把所有服务器的本地硬盘组织成一个虚拟存储资源池， 对上层应用提供块存储功能。 XXX ONEStor 分布式存储软件系统具有如下特点：

领先的分布式架构

XXXONEStor 存储软件的采用全分布式的架构：分布式管理集群，分布式哈希数据分布算法， 分

布式无状态客户端、 分布式 Cache 等，这种架构为存储系统的可靠性、 可用性、 自动运维、 高性能等方面提供了有力保证。

ONEStor 逻辑上可分为三部分： OSD、 Monitor 、 Client 。

在实际部署中， 这些逻辑组件可灵活部署， 也就是说既可以部署在相同的物理服务器上， 也可以根据性能和可靠性等方面的考虑， 部署在不同的硬件设备上。 下面对每一部分作一简要说明。

OSD： Object-based Storage Device

OSD 由系统部分和守护进程（ OSD deamo）n 两部分组成。 OSD 系统部分可看作安装了操作系统和文件系统的计算机， 其硬件部分包括处理器、 内存、 硬盘以及网卡等。 守护进程即运行在内存中的程序。 在实际应用中， 通常将每块硬盘（ SSD 或 HDD） 对应一个 OSD， 并将其视为 OSD 的硬盘部分， 其余处理器、 内存、 网卡等在多个 OSD 之间进行复用。 ONEStor 存储集群中的用户都保存在这些 OSD 中。 OSDdeamon 负责完成 OSD 的所有逻辑功能， 包括与 monitor 和其他 OSD（事实上是其他 OSD 的 deamon） 通信以维护更新系统状态， 与其他 OSD 共同完成数据的存储和维护， 与 client 通信完成各种数据对象操作等等。

Monitor ：

Monitor 是集群监控节点。 Monitor 持有 cluster map 信息。 所谓 Cluster Map ， 略的说就是关于集群本身的逻辑状态和存储策略的数据表示。 ONEStor Cluster Map 包括 Monitor map 、osd map、pg map、 crush map 等， 这些 map 构成了集群的元数据。 总之， 可以认为 Monitor 持有存储集群的一些控制信息， 并且这些 map 信息是轻量级的， 只有在集群的物理设备（如主机、硬盘） 和存储策略发生变化时 map 信息才发生改变。

Client ：

这里的 Client 可以看出外部系统获取存储服务的网关设备。

client 通过与 OSD 或者 Monitor 的交互获取 cluster map， 然后直接在本地进行计算， 得出数据的存储位置后， 便直接与对应的 OSD 通信，完成数据的各种操作。 在此过程中， 客户端可以不依赖于任何元数据服务器， 不进行任何查表操作， 便完成数据访问流程。 这一点正是 ONEStor 分布式存储系统可以实现扩展性的重要保证。

客户的数据到达 Client 后， 如何存储到 OSD 上。

File ： 此处的 file 是对用户或者应用而言的， 指用户或者应用需要存储或者访问的文件。如果将 ONEStor 作为对象存储的后端， 这个 file 也就对应于应用中的 “对象”， 也就是用户直接操作的 “对象”。

Object ： 此处的 object 是 ONEStor 内部定义的“对象” 。 object 的大小用户可以自行配置（在配置文件中设置， 通常为 2MB 或 4MB）。

当上层应用向 ONEStor 集群存入 size 较大的 file 时， 需要将 file 切分成统一大小的一系列 object （最后一个的大小可以不同） 进行存储。 为避免混淆， 在本文中将尽量避免使用中文的“对象” 这一名词， 而直接使用 file 或 object 进行说明。

PG:（ Placement Group） PG 是一个逻辑概念， 其作用是对 object 的存储进行组织和位置映

射。这样便在 object 和 osd 之间提供一个中间映射层，即 object->pg->osd 。某个 object 通过算法映射到某个确定的 pg， 这个 pg 再通过某种算法映射到一组确定的 osd（其个数和副本或纠删码配置有关， 具体见后面章节描述） 。 从数量上看，一般 object 数量远大与 pg 数量， pg 数量（一般比 osd 大两个数量级） 远大于 osd 数量。 PG 的概念类似于一致性哈希算法中的虚拟节点，引入 PG 后， 可以在总体上大大减少每个 osd 相关的元数据的数量。

下面对寻址流程进行简要说明。

1 ，File->Object 映射:（ino,ono ）->oid 这个映射比较简单，就是将用户要操作的 file ，映射为 ONEStor 能够处理的 object 。其本质就是按照配置文件定义的 object 大小对 file 进行切分， 相当于 RAID 中的条带化过程。 这种切分的好处有二：

一是让大小不限的 file 变成 size 一致、 可以被存储集群高效管理的 object ； 二是让对单一 file 实施的串行处理变为对多个 object 实施的并行化处理， 以提高读写性能。

对于要操作的 File ， Client 将会从 Monitor 获得全局唯一的 inode number ， 即 ino 。 File 切分后产生的 object 将获得唯一（在 File 的范围内） 的 object number ， 即 ono。 Ono 的编号从 0 开始，依次累加。 oid 就是将 ono 连缀在 ino 之后得到的。 容易看出， 由于 ino 的全局唯一性（通过 Monitor 获得） ， oid 同样具备全局唯一性。

2， Object -> PG 映射

在 file 被映射为一个或多个 object 之后， 就需要将每个 object 独立地映射到一个 PG 中去。 这个映射过程也很简单， 其计算公式是：

hash(oid) & mask -> pgid

或者更加明显的表示成：

hash(oid) mod (pgno) -> pgid

上式中， pgno 表示配置的 pg 数量， 一般为 2 的整数次幂。 整个计算由两步组成。 首先是使用 ONEStor 系统指定的一个特定的哈希函数计算 oid 的哈希值（这个值将具备近似均匀分布的特性） 。 然后，将这个伪随机值对 pgno 取模， 就得到了 pgid 。 这样， pgid 的取值范围是从 0 到 pgno-1 。 由哈希函数的伪随机特性， 容易想见， 大量的 oid 将近似均匀地映射到不同的 pgid 上。

3， PG -> OSD 映射

第三次映射就是将作为 object 的逻辑组织单元的 PG 通过 CRUSH 算法映射到一组 OSD 集合。集合中具体的 OSD 个数一般为数据副本的个数。 比如， 用户配置了 3 副本， 那么每个 pg 将映射到 3 个 osd。

多副本可以大大提高数据的可靠性 （具体可见后面相关章节的说明） 。

相比于 “object -> PG ” 映射过程， CRUSH 算法要复杂的多。

通常情况下， 一个好的分布式算法至少满足如下的要求：

1 ， 数据的放置位置是 Client 计算出来的， 而不是向 Server 查出来的

2， 数据在存储体上满足概率均匀分布

3， 存储体动态变化时数据重分布时引入的数据迁移量达到最优或者次优除了这 3 点基本要求外， 一个好的算法还应该满足 ：

4， 可以基于指定的策略放置副本 ： 用于故障域隔离或其它要求

5， 在存储体引入权“ weight ” 的概念 ， 以便对磁盘容量 / 速度等进行区分

CRUSH 算法是 ONEStor 的核心算法， 完全满足上面提到的 5 点要求， 限于篇幅， 此处不对算法本身进行描述。 当系统中的 OSD 状态、数量发生变化时， cluster map 亦随之变化， 而这种变化将会影响到 PG 与 OSD 之间的映射， 从而使数据重新再 OSD 之间分布。

由此可见， 任何组件， 只要拥有 cluster map ， 都可以独立计算出每个 object 所在的位置（ 去中心化 ）。 而对于 cluster map ， 只有当删除添加设备或设备故障时， 这些元数据才需要更新， 更新的 clustermap 会及时更新给 client 和 OSD， 以便 client 和 OSD 重新计算数据的存储位置。

自动化运维

自动化运维主要体现在如下几个方面：

（ 1） 存储集群快速部署， 包括批量部署、 单节点增减、 单磁盘增减等。

（ 2） 设置监控报警系统， 发生故障时能快速界定问题、 排查故障。

（ 3） 根据硬件能力， 灵活地对集群中的节点进行灵活配置。

（ 4） 方便地进行故障域隔离， 以及对数据存储位置进行灵活选择。

（ 5） 在增删存储介质， 或存储介质发生故障时， 自动进行数据均衡。 保证集群数据的高可用性。

对于（ 1 ）（2） 两点， 详见“ ONEStor 管理系统” 章节， 在此不再赘述。

对于（ 3)， ONEStor 系统可以根据用户需求灵活地部署 Monitor 节点和 Client 节点。 一方面， 这些节点既可以部署在单独的物理服务器上， 也可以部署在和 OSD 相同的物理节点上。 另一方面， Monitor 和 Client 的节点可以根据用户的需求灵活地调整。 比如为了可靠性保证， 至少需要部署 3 个 Monitor 节点； 为了保证对象存储网关的性能， 需要部署过个 RGW （ Client ）节点。

对于（ 4)， 用户的需求主要体现在存储策略上， 比如在选用副本策略时， 用户可能希望不同数据副本存储在不同机架上面的主机上；

或者主副本存储在某个机架的主机上， 其它副本存储在另外机架的主机上； 或者主副本存储在 SSD 上， 其它副本存储在 HDD 上。 诸如此类等等。 这些需要都可以通过配置 cluster map 中的 rule set 进行灵活地配置。

对于（ 5)， 在增删存储介质， 或存储介质发生故障时， 系统会及时进行检测。 比如， 在磁盘发生故障时， ONEStor 会利用损坏数据在其他存储体上的副本进行复制， 并将复制的数据保存在健康的存储体上； 在增加磁盘时， 同样会把其他存储体的数据安排容量比例重新分布到新磁盘， 使集群的数据达到均衡。 在上述过程中， 完全不需要人工干预。

线性扩展能力

所谓线性扩展能力， 主要体现在两个方面： 一个是集群部署规模可以线性扩展， 另一个方面，随集群规模的扩展， 其性能要能够线性或近似线性扩展。

在规模上， 传统存储之所以在扩展能力上受限， 一个很重要的原因就是一般其采用集中式控制，并且在控制节点存储大量的元数据信息，从而使控制节点容易成为系统的瓶颈。对于 ONEStor 系统， 如上一章节所述， Client 节点通过 cluster map， 可以直接计算出数据的存储位置， 从而对 OSD 进行直接读写， 完全是分布式并行的； 而其元数据， 也就是 cluster map ， 是轻量级数据， 而且其更新的频率相对而言也是较低的。 这种架构就在理论上保证了 ONEStor 具备线性扩展能力。 当然， 除了集群架构和元数据的设计之外， ONEStor 在缓存设计， 节点数据迁移方式等方面同样满足线性扩展的要求， 具体见后面章节描述。 理论上， 存储集群的最大节点数量并没有限制； 实践中，已经有超过一百个节点的部署应用。

在性能上， 由“领先的分布式架构” 章节可知， Client 端的读写数据最终会被 CRUSH 算法打散， 以概率均匀的方式分布到各 OSD 上，从而集群整体的 IO 和 Throughput 能力是各节点能力的总和。 换句话说， 也就是集群的性能随节点数量的增加而线性增加。

高可靠性

（ 1） 多副本机制

对存储系统来说， 可靠性（ Reliability ） 一般指其对存储的数据无差错地保存能力， 一般以在一段时间内的不出错的概率来表示，比如 AMAZON 宣称， 其 S3 服务在一年的时间内其数据可靠性最高可以达到 1 1 个 9， 即 99.99999999%。

为了对数据存储获得高可靠性， 常用的方法就是多副本技术， 即把用户的数据在存储体中存放多份， 比如典型的 3 副本。 在这种情况下， 只有在 3 份数据全部丢失， 用户的数据才会真正丢失。 在 ONEStor 系统中， 数据的多副本分布示意图如下图所示。

一方面， 用户数据（为简便计， 用数字序号表示） 的不同副本放置到多个不同的磁盘， 具体放置到哪些磁盘由数据放置算法决定； 另一方面， 同一个磁盘会承载多个用户的数据。 在商业存储系统中， 如果某个磁盘发生了损坏， 系统为保证副本个数， 会将损坏磁盘所包含的用户数据利用其它磁盘的数据副本复制到其它可用磁盘（可能不止一个， 不同系统有不同算法） 。 当然，复制是需要时间的，不同的系统在不同条件下有不同时间， 其差异可能从数分钟到数十小时， 为后面的讨论方便起见， 这个时间我们简记为 Tr 。

对上面的例子来说， 存储系统的数据可靠性等同于系统中持有的三个副本数据同时丢失。 这里所谓的同时并不是指数据所在的磁盘确切地在相同的时间损坏， 而是指在 Tr 时间段内， 三个副本所在的磁盘同时损坏。

我们知道， 对一般的电子元件来说， 其寿命一般符合指数分布。

实践表明， 磁盘的寿命同样满足此规律。 为了提高存储系统的可靠性，一个重要的方法就是想办法减小 Tr 时间， 也就是说， 在某个磁盘发生损坏时， 要在尽量短的时间内将其上的数据恢复到其它磁盘。

由前面的描述我们知道， 在 ONEStor 系统中， 对一个确定的 object ， 会映射到一个确定

的 PG， 这个 PG 又会映射到一组（对 3 副本来说， 就是 3 个） 确定的 OSD。 上述步骤中的每一个映射都是伪随机的。 如果从磁盘的角度观察， 我们会看到对于一个确定的 OSD， 它一般包含若干个 PG（一般在 1 00 这个数量级， 并且每个 PG 中包含着

若干的 object ）， 对着其中的每个 PG 而言， 都会存在 2 个另外的 OSD，含有相同的 PG。如果我们把具有相同 PG 的 OSD 称为“关联” 关系的话，那么对于一个特定的 OSD， 可能系统中会存在几十到上百个 OSD 与其存在关联关系，当然，这个前提是存储系统中首先要有这么多的 OSD。

这样， 当某个 OSD 失效时， 首先 ONEStor 会侦测到这个 OSD 故障，并更新 cluster map 。此时， 失效 OSD 存在关联关系的每一个 OSD 会重新计算出一个新

OSD 来代替这个失效的 OSD， 并在新的 OSD 上写入一份新的副本。 由 CRUSH 算法的伪随机性不难想象， 不同的关联 OSD 计算出的新的 OSD 很可能是不同的。 换句话说， 当一个 OSD 损坏时，其上的数据并不是全部简单地拷贝到某一个新的 OSD 上， 而是在系统中由众多的 OSD 共同承担，每个 OSD 将其中的一部分数据恢复到新的 OSD 上。打个通俗的比喻就是“一人有难，八方支援” 。在这样的分布式并行数据恢复机制下， 会比传统的单一节点恢复节省几十到上百倍的时间， 从而在系统的可靠性上得到极大的提升。

对于 ONEStor 系统， 理论计算和模拟实验表明， 在典型的 3 副本机制下， 在不少于 30 个磁盘的系统中， 数据在一年内的可靠性可以达到 1 1 个 9 的水平。

除了数据的可靠性， 其 Monitor 节点也是分布式部署的， 同样不存在单点故障问题。 这样在 ONEStor 系统中， 不论是数据还是元数据，都不存在单点故障， 并达到极高的可靠性。

（ 2） 数据一致性

所谓一致性， 略地说， 就是分布式系统通过副本控制协议，使得从系统外部读取系统内部各个副本的数据在一定的约束条件下相同。 依据一致性的强弱条件不同， 副本一致性可以分成若干级别，如强一致性、 单调一致性、 会话一致性、 最终一致性等。

在 ONEStor 系统中， 一方面要保证元数据的一致性； 另一方面要保证用户数据的一致性。

元数据的一致性， 是指多个 Monitor 之间关于这个集群的 cluster map 要保持一致性。 因为不论 client 还是 OSD， 都要依据 cluster map 来定位和分布数据， 故而元数据的一致性是必须的。 为了达到此点， ONEStor 的 Monitor 之间采用了 Paxos 和 Lease 机制来保证元数据的一致性问题。 Paxos 和 Lease 机制， 都有公开的文献讨论， 在此不再赘述。

对于用户数据的一致性， ONEStor 系统保证数据的强一致性， 所谓强一致性， 就是任何用户或节点都可以读到最近一次成功更新的副本数据。 强一致性是程度要求最高的一致性。

ONEStor 系统实现了用户数据的强一致性。

其基本原理如下：

假定文件以 3 副本写入到 ONEStor 集群中， 则寻址过程中每个 object 将被映射到 3 个不同的 OSD（注意， 这 3 个 OSD 是有顺序的，其顺序由 CRUSH 算法决定） ， 这 3 个 OSD 依次称为 Pirmary OSD，Secondary OSD， Tertiary OSD 。 对于其中的某个 object ， 其写入流程如下：

在 Client 本地计算出三个 OSD 后， 将直接和 Primary OSD 通信，发起写入操作 （步骤 1）。

Primary OSD 收到请求后， 分别向 SecondaryOSD 和 Tertiary OSD 发起写入操作（步骤 2、 3）。当 Secondary OSD 和 Tertiary OSD 各自完成写入操作后， 将分别向 Primary OSD 发送确认信息（步骤 4、 5）。 当 Primary OSD 收到其他两个 OSD 的写入确认后， 并自己也完成数据写入， 则向 client 确认 object 写入操作完成（步骤 6）。

良好的性能

对用户来说， 存储系统的性能体现在两个方面： 一个是从 Client 角度看， Client 可以从系统获得的性能； 一个是从存储集群的角度看， 存储集群的供给能力。

首先， 从 client 角度看， 比如利用集群的块存储 RBD。 此时，LUN（也就是 RBD 块） 会根据 CRUSH 算法伪随机地分散在集群的所有磁盘。 这个分布是通过集群自动完成， 无需手动配置。由于每个 LUN 可以使用整个集群的磁盘性能， 因此整个集群能够提供更高的性能。

在 ONEStor 集群中， LUN 默认划分大小是 4M（可配置） object ， 比如一个 1GB 大小的 LUN，会被划分成 256 个 object ， 这些 object 分散在不同的 OSD 上。 这样在读写 LUN 时， 就会充分利用集群的整体性能，提升 IOPS 和 Throughput 。

存储集群的性能取决于两方面： 一方面是单节点的能力， 另一方面是系统的扩展能力。 如前所述， ONEStor 系统的性能可以随节点的规模而线性扩展， 所以对第二点来说， 已经达到了最大化。 对于单节点的能力， ONEStor 在系统设计和硬件配置方便实现了足够的灵活性，从而可以表现出良好的性能。

对传统的 HDD 来说， 受寻道能力的限制， 单盘的随机读写能力一般不超过 ***IOPS 。 SSD 的出现， 使得在 IOPS 上的能力相比于 HDD 有了大幅的提升， 一般可以提升 2 个数量级以上， 从在在当前对 IOPS 有较高需求的应用（如数据库、 VDI 等） 中得到了广泛使用。 另一方面，当前 SSD 在容量、 价格、 使用寿命等方面和 HDD 相比还有一定的差距， 所以针对不同的场景和需求，一个良好的存储系统应该可以进行灵活的配置。 具体来说：

ONEStor 系统支持的硬盘类型包括： 全 HDD、 SSD+HD 混 D 合组网、全 SSD。

在 SSD+HDD 混合组网模式下， ONEStor 系统既可以将 SSD 作为 Cache 使用， 也可以将 SSD 和 HDD 放到不同的 pool ， 做分层存储使用。

在混合模式下， 既可以发挥 SSD 的 IOPS 和 Throughput 的优势，又可以发挥 HDD 的容量和价格优势， 是目前广泛采用的存储架构。

统一的存储业务

从存储系统的业务供给能力角度看，不同的存储系统可以提供所谓的块存储(FC SAN/IP SAN)、文件存储 (NAS)、 对象存储等不同类型。 假如用户有多重应用， 就需要购买不同的存储系统。ONEStor 基于 Ceph 开发，因为 Ceph 本身提供了块、对象、文件等多种不同的接口，故而 ONEStor 也可以对用户提供不同的存储接口。

ONEStor 系统的软件逻辑分层：

底层存储服务集群， 这一层是一个对象存储系统， RADOS 采用 C++开发。

库函数接口 ： 这一层的功能是对底层存储服务进行抽象和封装， 并向上层提供 API（包括 C

和 C++、 Java、 Python、 Ruby 和 PHP 的支持。

高层应用接口 ： 这一层包括了三个部分： 对象服务、 块设备服务、 文件服务等三部分应用层 ： 这一层就是不同场景下对于 ONEStor 各个应用接口的各种应用方式。

从用户的角度， 一个存储集群就可以满足用户不同的存储应用。

ONEStor 对硬件设备要求服务器

最少部署 三台服务器。

硬盘

系统盘： 必配， 至少 2 块硬盘。 2 个硬盘做 RAID1 用来安装 ONEStor 等系统软件， 不作为数据盘； 系统盘建议使用 SAS 盘， 容量、 转速没有特殊要求。

数据盘： 必配， 至少 1 块硬盘：

1 、 转速建议 1 OK 以上， 单盘做 RAIDO 条带化；

2、 ONEStor 使用副本机制 (2~N 副本) 或纠删码机制保障可靠性。

如果使用 N 副本， 则可用容量是裸容量的 N 分之一。 建议使用 2-3 副本， 保持较好的性价比。 如果对存储效率都有比较高的要求， 也可以采用纠删码技术， 此时对 CPU 要求有所提高。

3、 不同节点硬盘类型（容量、 转速） 可以不同， 但为保证最佳性能， 需要采用一定的配置策略。 在一般项目中， 为简化起见， 建议不同节点配置相同类型的硬盘。 为保证系统性能， 建议配置 1 0000rpm 的硬盘。

SSD

SSD 为系统提供快速写日志功能及缓存加速功能， 建议每台服务器 SSD 硬盘容量与机械硬盘的容量比为 1 :5 。

内存

根据服务器配置的数据盘容量计算 ONEStor 占用内存容量： 51 2M 内存/TB 磁盘容量。 例如某服务器节点配置 8 块 1 T 的数据盘， 那么 ONEStor 占用内存容量为： 8*51 2M = 4G。 注意： 服务器还需要配置足够的内存供虚拟机使用。

RAID 控制器

必配， XXX FlexServer 服务器默认已自 带硬件 Raid 卡。 其他品牌服务器需确认形态及兼容性。 RAID 卡缓存推荐配置不少于 2G。 如果 Raid 卡没有电源保护， 则关闭 Cache。

网络

至少配置 3 个网口， 分别对应存储内网、 管理网、 业务网， 其中存储内网为万兆网卡， 其他可千兆； 为进一步提升可靠性及性能， 建议网口采用冗余配置， 共 6 个网口（ 2 个万兆， 4 个千兆） 。 如果还要求提供外部存储服务， 则需要另配网卡（千兆或者万兆均可） 。

以太网交换机

在服务器节点较少的时候， 多张网络可以共用交换机， 通过 VLAN 隔离； 存储内网交换机必须为万兆端口。

管理系统的特点

无中心管理架构设计

XXX ONEStor 的管理系统称为 Handy。

为了满足管理平台的高可用性（ HA） 特性， 现有技术方案一般都是采用 HA 工具（如 keepalived ） 实现， 如图 1 所示， 管理平台分为活动节点和备用节点两部分， HA 工具会在活动节点 A 上配置一个 VIP（本例中为 IPV1)， 用户通过 IPV1 访问管理平台时， 请求的是实际 IP 地址为 IPA 的节点 A。

当活动节点 A 出现故障时， HA 工具通过各个节点之间的心跳检测可以感知到， 这时候会将 VIP 配置到备用节点 B 上， 并将节点 B 标记为活动节点， 用户这时候通过 IPV1 访问管理平台时， 实际访问的已经是 IPB 所在的节点 B。

现有技术的缺点主要是：

1 、 管理平台数据库中的信息要跟集群中的信息进行同步。 一方面， 假如不通过管理平台，而是通过命令行的方式增加配置到集群中，管理平台就不能感知到， 所以需要定时同步集群数据到管理平台上。

另一方面， 管理平台数据库的引入也增加了系统的复杂性和失效风险。

2、 活动节点与各个备用节点之间的所有数据（包括数据库、 监控信息、 日志信息等） 都要进行同步。

3、 需要额外的 HA 软件（如 keepalived ） 来实现管理平台各节点之间的心跳检测， 增加了网络负担。

Handy 针对以上缺点， 重新设计了管理架构， 充分利用 ONEStor 集群本身的 HA 特性， 实现了管理节点和存储节点的深入融合， 以达到以下目的：

1 、 系统的配置和状态信息直接从集群中获取， 不需要保存到单独的数据库中， 解决了数据库与集群数据的一致性问题。

2、 活动节点与所有的备用节点之间不需要同步任何数据， 包括数据库、 日志信息等， 大大减少了网络带宽的占用和数据同步的复杂度。

3、 利用 ONEStor 自身的 HA 机制， 就可以实现 VIP（虚拟 IP ） 从管理节点到健康管理节点的自动切换。

需要说明的是， Handy 节点既可以部署的独立的物理服务器上，也可以和 ONEStor 部署在相同的物理服务器上， 以便用户根据集群的规模和特定要求灵活选择。

场景化设计

对一般用户来说， 对存储系统进行配置还是一项比较繁琐的工作， 尤其是对一些参数的选择更是不易。为了最大限度的简化存储配置管理，Handy 对 ONEStor 主要的应用场景进行了总结，在不同的场景中对一些原本需要用户输入的参数进行智能计算，这样用户只需要根据业务需要选定场景， 就可以很容易地完成相关配置。 其基本配置页面如下图所示：

管理系统的主要功能

首次登录 Handy 管理系统， 需要先创建一个 ONEStor 集群， 并通过： 基本信息、 场景选择、

增加机架、 增加主机、 确认信息等步骤完成集群的创建。 在以上步骤中， 只需要根据向导即可轻松完成 ONEStor 集群的部署。

Handy 管理系统分为： 系统概览、 集群管理、 存储管理、 运维监控、 系统管理， 共五部分。

系统概览 ： 主要描述 ONEStor 集群的整体状态， 包括：

1， 主机、 硬盘、 监控器、 虚节点等健康状态

2， 集群整体的 IOPS 和存储容量使用量

3， 群的告警信息

4， 集群的物理拓扑展示

其界面如下图所示：

集群管理 ： 分为主机管理和集群拓扑两部分。

在主机管理中， 可以选择手动部署或自动部署将新的主机加入到集群中。 在集群中可以显示所有主机的信息， 包括硬盘数量和状态、存储使用率、 CPU 使用率和内存使用率等。

集群拓扑中， 集群中主机的形态以直观的拓扑显示在管理界面中， 当鼠标移至机架、 服务器、硬盘上时会有具体的信息显示物理设备的状态； 当硬盘出现故障时， 硬盘灯将由绿色变为红色。

存储管理 ： 分为 Pool 管理、 块存储管理、 对象存储管理等。

Pool 管理主要完成根据不同应用场景创建不同的存储池， 并制定存储池的创建策略， 比如副本策略、 SSD 策略、 对象网关等。

块存储管理可以完成对块的创建、 修改、 删除、 快照、 快照管理、克隆操作。

对象存储管理主要是为对象存储业务创建对象网关。

运维监控 ： 运维监控页面可以查看各个主机和硬盘的资源占用情况， 包括 CPU、 内存、 硬盘吞吐、 硬盘时延、 硬盘 IOPS 和硬盘容量等。

系统管理 ： 主要包括告警管理、 日志管理、 用户管理、 用户组管理等。

13.2.5 整体关键技术虚

13.2.5.1 网络虚拟化技术设计

全方位虚拟化能力

IRF2（Intelligent Resilient Framework2 ， 第二代智能弹性架构）

全系列数据中心交换机产品全部支持 IRF2 技术， 最多将 4 台高端设备虚拟化为一台逻辑设备， 在可靠性、 分布性和易管理性方面具有强大的优势；

可靠性： 通过专利的热备份技术， 在整个虚拟架构内实现控制平面和数据平面所有信息的冗

余备份和无间断的数据转发，极大的增强了虚拟架构的可靠性和高性能，同时消除了单点故障，避免了业务中断；

分布性： 通过分布式跨设备 路聚合技术， 实现多条上行 路的负载分担和互为备份， 从而提高整个网络架构的冗余性和 路资源的利用率；

易管理性： 整个弹性架构共用一个 IP 管理， 简化网络设备管理， 简化网络拓扑管理， 提高运营效率， 降低维护成本。

MDC （Multitenant Devices Context ， 多租户设备环境）

数据中心交换机产品可以通过 MDC 技术可以实现 1： N 的虚拟化能力， 即一台物理交换机虚拟化成 N 台逻辑交换机， 最多可虚拟为 1 6 台逻辑交换机， 满足多客户共享核心交换机的需求；通过单块板卡的端口划分到不同 MDC ， 既可以充分利用核心交换机的能力， 又降低了用户的投资成本， 使用 MDC 技术实现了对业务的安全隔离。

路聚合技术

路聚合在增加 路带宽、 实现 路传输弹性和工程冗余等方面是一项很重要的技术。

他通过将多条低带宽端口通过协议逻辑上捆绑成一条高带宽的 路， 在此过程中不改变现有网络设备以及原有的布线。多条 路捆绑成一条逻辑 路，路带宽增加；被捆绑的 路间负载平衡，可提高额外的容错性能。 只需要在网络设备上配置， 灵活性高。

13.2.5.2 服务器高可用技术设计

XXX CAS 高可靠性（ HA） 技术

XXX CAS CVM 虚拟化管理平台将一组服务器主机合并为一个具有共享资源池的集群， 并持续对集群内所有的物理主机与虚拟机运行状况进行检测， 一旦某台服务器主机或虚拟机发生故障，XXXCASHA 软件模块会立即响应并在集群内另一台服务器主机上重启所有受影响的虚拟机。

相关术语

CVK 节点： 安装了 CVK 虚拟化内核系统的服务器节点， 承载 CAS 虚拟化内核的实现。 在 HA 实现中， 每个 CVK 节点都会安装一个 HA 的后台进程， 用于检测主机和虚拟机的故障。

CVM 节点：安装了 CVM 虚拟化管理平台的服务器节点，为整个虚拟化环境的集中管理平台，包括对集群 HA 的管理， 在 HA 的实现中， CVM 节点管理集群内的所有 CVK 节点， 并建立与所有 CVK 之间的心跳。

网络心跳（ Network HeartBeat ） ： 一种定期发送的心跳报文， 来检测管理网络中 CVK 节点的 HA 进程是否运行正常。 网络心跳发送的定时间隔可以调整，支持 5~1 20 秒的设置， 默认的网络心跳周期为 1 0 秒。

存储心跳（ Store HeartBeat ） ： 存储心跳用于检测在存储网络中 CVK 主机是否能够正常访问与它连接的共享存储池， 主机的故障判断基于该主机是否能够正常访问它所连接的共享存储池。存储心跳发送的定时间隔可以调整， 支持 5~1 20 秒的设置， 默认的存储心跳心跳周期为 1 0 秒。

物理服务器主机 HA 工作原理

物理主机的 HA 实现过程分成三个步骤：

1 ） 主机故障检测

CAS CVK 服务器主机故障分成两种情况：

整个物理主机硬件故障导致无法启动或者宕机。

主机连接的某个共享存储池无法正常访问。

第一种情况下， 则 CAS HA 模块会将此物理主机上的所有虚拟机迁移到其他正常运行的主机上；

第二种情况下， 该主机将被隔离并重启 （主机隔离重启由存储服务软件模块实现） ， 如果重启完成主机恢复运行后， 该共享存储池还是无法正常访问， 则 CAS HA 模块会将部署到该共享存储池的虚拟机迁移到其他正常的主机上（该主机其他访问正常的共享存储池上的虚拟机不受影响），如果该主机隔离重启后， 长时间未恢复正常运行， 该时间超过 HA 进程的主机故障检测的最大周期， 则该主机上的所有虚拟机都将迁移到其他运行正常的主机上。

主机的故障由 CVK 节点实现， CVK 节点通过存储心跳机制来检测该主机是否运行正常。 存储心跳的检测实现也分两种情况。

第一种情况， CVK 节点与 CVM 节点的管理网络连接正常：

当主机挂载某一共享存储池时， CVK HA 进程就启动一个独立线程进行对该共享存储池进行存储心跳检测， 存储心跳检测正常时， 说明该存储池访问正常， 部署在该共享存储池上的虚拟机不受影响。 当 CVK 节点连续三次检测到存储心跳异常时， 则通过消息上报给 CVM 节点， 报告该存储池故障。 CVM 节点接收到 CVK 节点发送的存储池故障消息后， 将查询该存储池部署的虚拟机信息， 并将这些虚拟机进行故障迁移。

在管理网络正常的情况下， 若发生主机故障， 则经过三个存储检测周期后，虚拟机就会发生迁移。

第二种情况， CVK 节点与 CVM 节点的管理网络连接断开：

当 CVM 节点感知到与 CVK 节点 1 的网络断开时， 此时 CVM 节点将选择同一个 HA 集群中的挂载了相同的共享存储池的其他 CVK 主机， 如上图中的 CVK 节点 2， 该节点与 CVM 节点的管理网络通信正常， CVM HA 进程发送消息到该 CVK 节点 2 的 HA 进程， 请求返回 CVK 节点 1 的存储心跳检测结果。 CVK 节点 2 获取 CVK 节点 1 与该主机挂载的共享存储的存储心跳检测结果后， 将该信息通过消息返回给 CVM 节点。 CVM 节点判断出 CVK 节点 1 的存储心跳检测结果后， 后续的处理流程就和第一种情况一致： 如果该 CVK 主机 1 与某个存储池连续三次出现存储检测异常， 则将受影响的虚拟机迁移到其他正常的主机上。

注意： 如果 CVM 节点无法找到该 HA 集群中其他主机用于获取 CVK 主机 1 的心跳结果， 此时虚拟机无法迁移， 用户需要排查管理网络或者服务器和共享存储的配置是否正确。

如果物理主机故障导致无法正常运行或者宕机， 则此时 CVM 节点无法获取该主机所有挂载的共享存储池的存储心跳检测结果， 此时该主机上所有的虚拟机都会进行故障迁移。

前面描述的 CVM 节点与 CVK 节点的管理网络连接状态是通过集群网络心跳机制来获取的， CAS

HA 集群的网络心跳实现为点到多点的组网模式，所有的 CVK 主机只与 CVM 主机建立网络心跳检测。集群中的 CVK 主机启动 HA 功能后， 此时将启动网络心跳线程， 该线程定时发送网络心跳报文到 CVM 节点， CVM 节点接收后回复心跳响应。

HA 集群主机的网络心跳检测机制

如果 CVM 节点连续三次未收到 CVK 节点的网络心跳报文， 则将该 CVK 节点的状态置为管理网络断开状态。

主机隔离

主机隔离的作用为防止故障的物理主机异常访问共享存储， 破换用户的数据。

主机隔离的实现分两个步骤：

CVK HA 进程检测到某个共享存储故障后， 通过发送消息到 CVM 节点， 通告存储心跳检测故障，并将部署在该共享存储下的虚拟机关闭， 防止运行的虚拟机破换共享存储上的用户数据。

主机检测到某共享存储持续一段时间无法正常连接后， 将主机自身重启。

虚拟机迁移

集群 HA 启动后， 当某物理主机故障后， 该主机上的虚拟机将迁移到其他运行正常的主机上。虚拟机的磁盘必须使用共享存储，否则无法迁移。

虚拟机迁移分两种：

在检测到物理主机故障后， 原来在该主机上运行的虚拟机将自动选择在其他一台正常的物理主机上启动。

离线的虚拟机在检测到主机故障后， 并不会自动迁移， 这些虚拟机只有当用户在 CVM 控制台界面上点击启动时， 此时会才选择在其他正常运行的物理主机上启动。

虚拟机的迁移时， CASHA 将根据当前集群中 CVK 主机的 CPU 利用率、 内存利用率、 主机运行的虚拟机个数等信息， 选择一台最优的物理主机进行迁移。

虚拟机 HA 工作原理

虚拟机的检测周期为 30 秒（不可调整） 。 集群 HA 启动后， CVK 主机 HA 进程根据虚拟机的检测周期会对每个虚拟机进行故障检测，连续三次检测到虚拟机故障后， 就通过消息上报给 CVM 节点， 报告虚拟机故障， CVM 节点将该故障的虚拟机迁移到其他正常运行的 CVK 节点。

CVK 主机检测到虚拟机故障时，会首先尝试一次在本主机上重新启动一次，如果启动失败，则再上报给 CVM 节点， 报告虚拟机故障； 如果启动成功， 则不再上报该虚拟机故障。

如果该 CVK 主机与 CVM 主机之间的管理网络中断， 由于与 CVM 节点无法进行消息通信， 则该虚拟机无法迁移， 用户需要排查管理网络的问题。 当管理网络恢复正常时， 如此时虚拟机还是故障， 则该虚拟机将会被迁移到其他正常运行的主机上。

技术特色总结

XXX CAS HA 技术有效的解决了目前其它高可用性解决方案面临的问题：

当物理服务器发生硬件故障时， 所有运行于该服务器的虚拟机可以自动切换到其它的可用服务器上， 相对传统的双机容错方案，XXX CAS HA 可以最大程度减少因硬件故障造成的服务器故障和

服务中断时间。

不同于其它 HA 的双机热备方式， 所有参与 HA 的物理服务器都在运行生产系统， 充分利用现有硬件资源。 同时， 对众多的操作系统和应用程序， XXX CAS 提供统一的 HA 解决方案， 避免了针对不同操作系统或者应用， 采用不同的 HA 方案带来的额外开销和复杂性。

通过 XXX CAS HA， IT 部门可以：

为没有容错功能的应用提供冗余保护

传统意义上 HA 实现很复杂并且价格昂贵， 多用于关键性的服务或应用，而 XXX CAS HA 为所有的应用程序提供了高性价比的 HA 解决方案。

为整个 IT 环境提供“第一条安全防线”

不同于其它基于操作系统和应用的 HA 实现方式， XXX CAS HA 为 IT 系统提供了更统一、 更易于管理的高可用性解决方案。 XXX CAS 用最少的成本和最简单的管理方式为所用的应用提供了最基本的冗余保护功能。

综上所述， XXX CAS HA 解决方案的技术特点总结如下：

自动侦测物理服务器和虚拟机失效

XXXCAS 会自动的监测物理服务器和虚拟机的运行状态，如果发现服务器或虚拟机出现故障，会在其它的服务器上重新启动故障机上所有虚拟机， 这个过程无需任何人为干预。

虚拟机自动重新启动

通过在其它的物理服务器上重新启动虚拟机， HA 可以保护任何应用程序不会因为硬件失效而中断服务。

智能选择物理服务器

当与 XXX CAS 动态负载均衡功能共同使用时， XXX CAS HA 可以根据资源的使用情况， 为失效物理服务器上的虚拟机选择能获得最佳运行效果的物理服务器。

13.2.5.3 数据库高兼容性设计

云平台支持如下数据库： My SQL、 SQL SERVE、RORACLE 以及国产化数据库。 用户使用功能包括：

1 ．通过浏览器申请， 审批可自动创建分配数据库资源。

2. 浏览器即可安全、 方便的进行数据库管理和维护。

3. 支持多租户， 租户之间网络隔离。

4. 支持用户资源隔离 ,CPU,Memory,IO 隔离。

5. 提供高可靠， 高可用的数据库服务， 故障时可快速切换。

6. 支持自定义的备份策略保障数据的安全性。

7. 支持自定义的 IP 访问白名单的设置。

8. 支持用户的前端行为审计， 数据库日志查询及分析。

13.2.5.4 存储高可用技术设计

全网状控制器集群架构

存储服务器采用全网状控制器集群架构，通过一个高带宽、低延迟特性的背板，将经济高效、模块化、可升级的组件统一成一个具有高可用性的、可自动均衡负载的集群。其独特的架构使得单台性能大大超越传统的存储。

独特的双分类处理单元

使 StoreServ 可以支持混合工作负载，从而减轻性能负担，降低了传统阵列的成本。使用 StoreServ，交易数据处理和吞吐量密集型工作负载再也不必争用相同的存储资源。它是通过使用相关的数据缓存，在每个控制器节点内并行迁移数据；同时，使用 IntelCPU 和相关的控制缓存来处理元数据而实现的。

其具体工作原理如下：当不同类型的数据同时进入存储控制节点时，不同的控制器和缓存处理不同的工作负载，控制处理器处理不同数据的控制信息，迅速计算出其存放规则和地点，而 ASIC 芯片负责数据的实际搬运工作。两种不同架构的处理器高效的完成各自的任务，并发工作，大大提高了存储处理不同数据类型的效率。

业务连续性

传统的存储只能为一个存储卷创建 8 个或者更少的快照，其快照往往也需要预留一定的空间，所以传统的快照技术不能满足对于一天内多个时间点的状态保存，同时也会消耗额外不必要的空间。

存储可以提供一个逻辑卷多达 500 个的快照，同时不需要预留空间，做到真正的按需分配，大大节省了存储的空间。提高了存储的利用率。对于一些需要查询的业务，往往可以定时的采用快照技术，将快照卷挂载给查询主机来使用，提高了应用的灵活性。

对于未来可扩展的容灾架构，采用统一的存储平台，可以实现精简配置的双节点架构和多节点架构之间的无缝容灾，同时也是业界少数的支持三点容灾的厂家。客户无须为无法对传统的中端和高端存储容灾而烦恼。如下图：不同的存储平台之间可以进行无缝的三点容灾，主存储 A 和距离较近的存储 B 进行同步复制，和较远的存储实 C 行异步复制，当主存储 A 和异步复制的存储 C 间的 路中断时，B 存储自动和远端存储发起同步，达到容灾的持续性。

13.2.5.5 KVM 虚拟技术设计

基于定制化的开源虚拟化 KVM 虚拟化解决方案，国产化程度更高，更经济。整体由计算服务器、存储器网络和阵列、IP 网络、管理服务器等组件组成。

KVM（Kernel-based Virtual Machine），是一个开源的系统虚拟化模块，自 Linux 2.6.20 之后集成在 Linux 的各个主要发行版本中，包括 RedHat、CentOS、Ubuntu 等 Linux 系统均支持 KVM 虚拟化。目前，Openstack+KVM 的虚拟化架构，已逐渐成为与 VMware 匹敌的主流选择。

KVM 是一个独特的管理程序，通过将 KVM 作为一个内核模块实现，在虚拟环境下 Linux 内

核集成管理程序将其作为一个可加载的模块， 可以简化管理和提升性能。 在这种模式下， 每个虚拟机都是一个常规的 Linux 进程， 通过 Linux 调度程序进行调度。

KVM 群集由多台安装了 KVM 的物理服务器组成， 通过虚拟化管理器， 实现完整的平台虚拟化功能。

1、 完备的虚拟机生命周期管理：

支持虚拟机的创建、 修改、 启动、 暂停、 恢复、 休眠、 重启、关闭、 下电、 克隆、 迁移、 快照等常用功能， 同时支持通过管理界面的控制台远程连接到虚拟机。 所有的操作全部基于图形化配置界面。

2、 HA 高可用：

KVM 群集， 是由多台独立服务器主机聚合形成的集群， 不仅降低了管理的复杂度， 而且具有内在的高可用性 (High Availability,HA)， 从而为用户提供一个经济有效的高可用性解决方案。

HA 高可用对资源池中的虚拟机进行持续的监控， 统一在各个虚拟机之间维持“心跳” ， 当发现虚拟机失去“心跳” 的时候， 就会尝试在其它的服务器上重新启动失效的虚拟机。 HA 会保证任何时候当物理服务器发生宕机， 资源池中都有足够的硬件资源， 使失效的服务器中的虚拟机在其它的服务器上顺利启动。

3、 动态资源调度

在虚拟化和云计算环境中， 一旦客户将应用整合到负载较重的物理主机上， 虚拟机的资源需求往往会成为瓶颈， 全部资源需求很有可能超过主机的可用资源。 KVM 群集提供动态资源调度（ DynamicResource Scheduler ， DRS） 特性引入一个自动化机制， 通过持续地平衡容量， 将虚拟机迁移到有更多可用资源的主机上， 确保每个虚拟机在任何节点都能及时地调 用 相 应的资源。 即 便大量运行 SQLServer 的虚拟机， 只要开启了动态资源调整功能， 就不必再对 CPU 和内存的瓶颈进行一一监测。 全自动化的资源分配和负载均衡功能， 也可以显著地降低数据中心的成本与运营费用。

动态资源调度功能通过心跳机制，定时监测集群内主机的 CPU 和内存等计算资源的利用率，并根据用户自定义的规则来判断是否需要为该主机在集群内寻找有更多可用资源的主机，以将该主机上的虚拟机迁移到另外一台具有更多合适资源的服务器上，或者将该服务器上其它的虚拟机迁移出去， 从而保证某个运行关键业务虚拟机的资源需求。

4、 动态资源扩展

当一台虚拟机性能无法满足突发访问的需求时， KVM 群集可以自动的生成相同的虚拟机并发布至有资源空闲的物理服务器， 实现对高负荷业务的负载均衡。 当访问高峰过后， 也能将扩展资源收回。

13.3 IaaS 云服务方案

13.3.1 IaaS 云服务目录

13.3.1.1 计算存储网络服务目录

13.3.1.2 安全服务目录

13.3.2 云主机服务

云主机服务是市政务专有云计算在基础设施应用上的重要组成部分。 市政务专有云主机服务让您完全控制您的计算资源， 当您的计算资源需求发生改变时，可以按照市政务专有云提供的资源套餐随时进行计算资源的提升。 云主机服务整合了对于市政务专有云主机服务的常用管理功能， 通过云主机服务您可以看到您的云主机服务的配置信息， 而且可以对您的云主机服务执行重启、 关机、 启动、销毁、 远程连接等操作。 而且还可以随时查看最近八小时、 最近一天、 最近两周、最近一月 和最近半年您的云主机服务的监控信息， 监控信息包括： CPU 利用率、内存利用率、 磁盘 IO 和网络流量。

13.3.2.1 云主机概述

云主机是以虚拟机的形式运行的镜像副本。 基于一个镜像， 您可以创建任意数量的主机。 在创建主机时， 您需要指明 CPU 和内存的配置。 CPU、 内存的数量可以选择， 也允许在主机创建之后随时再行调整。 云主机的功能包括： 租户的云主机列表、 创建云主机、 云主机的操作列表、云主机的监控信息和费用报告。

云主机的列表： 租户登录 XXXloud 云服务管理平台后， 可以查看所有自己管理的主机列表，查看云主机信息包括： 所属用户、 名称、 状态、 内网 IP、 镜像模板、 规格类型、 网络、 运行时间和远程登录主机；

1）创建云主机： 根据镜像的分类选择镜像， 镜像列表包括镜像名称和描述；

2）创建云主机： 选择规格， 规格内容包括规格类型、 CPU、 内存和系统盘； 配置详情包括每小时和每天的总价：

3）创建云主机： 设置网络， 选择云主机接入的网络；

4）创建云主机： 基本配置， 需要输入云主机名称、 云主机数量和描述；

5）云主机操作列表， 用户可以管理所有的主机操作， 操作包括刷新、新建、 启动、 关机、

重启、 修改等；

6）帮助用户查看云主机的监控信息， 并可以查看包括所有的费用总统计和明细、 资源总统计和明细， 应用统计和性能统计。

13.3.2.2 云主机租户网络

提供了两种组网方式： 基础网络、 私有网络（基于 VLAN 或者 VxLAN） 。 前者是一个由系统维护的全局网络， 后者是组织管理员各自自行组建的网络。 基础网络的好处是简单、 无需用户做任何配置与管理， 即可直接使用， 但正因为它是全局网络， 所以其安全保障是依靠防火墙来实现的。 与之相对应， 私有网络需要组织管理员创建并管理。 但私有网络之间是 100%隔离的， 以满足对安全要求。 私有网络间使用路由器互联， 并可以控制政务外网地址对外映射。 组织管理员可以配置私有的防火墙来保证私有网络的安全。

云主机租户网络能够快速搭建您的私有云环境， 并使用丰富的工具进行自动化管理。

1 ）创建网络， 输入网络名称和描述信息：

2）配置网络， 在这里我们可以查看和修改私有网络包含的主机列表和端口列表；

路由器

路由器用于私有网络之间的互联，并提供以下附加服务：DHCP 服务、端口转发、隧道和 VPN。如果您还希望路由器能接入互联网， 请绑定一个公网 IP 给该路由器即可。

1）云管理服务台支持创建路由器；

2）配置路由器， 可以配置基本信息和租户信息：

3）路由器列表和操作列表， 包括 ID、 名称、 状态、 私网 IP 、 描述和创建时间等：

13.3.2. 自定义镜像

镜像是一个包含了软件及必要配置的机器模版。 作为基础软件， 操作系统是必须的， 还可以根据自己的需求将任何应用软件 （比如， 数据库、 中间件等）放入镜像中。 镜像分为两类。 其一是系统提供的， 称之为“系统镜像” ， 包括了各种 Linux 、 Windows 等操作系统， 各系统镜像的初始本地终端用户名和密码均可在各镜像的详情描述中找到。其二是用户通过捕获一个主机来自行创建的， 称之为“自有镜像” 。 系统镜像全局可见可用， 自有镜像只有用户本人可见可用。 帮助您一次性开通多台已完全拷贝相同操作系统及环境数据等的云服务器， 以便满足您弹性扩容的业务需求。

创建主机时可以从镜像模板中选择；

1）镜像模板列表， 包含两部分， 一部分为系统自定义的， 不能修改和删除， 另一部分为自由的镜像模板， 可以创建、 修改和删除。

2）创建镜像： 只能从自由列表中创建镜像模板， 包括名称、 描述、类型、 格式化、 最小

磁盘和最小内存等。

13.3.2.4 云主机特点

1 ） 多种性能规格， 可以自定义

2） 按小时计费

3） 快速部署

资源池并内置多种操作系统和应用标准镜像，需求无论是一台还是百台、Windows 还是 Linux ，均可实现瞬时供应和部署。

4） 高可用

国际品牌企业级服务器的高性能和可靠性， 内置的监控、 备机、 快照、 数据备份等服务确保故障的快速恢复。 提供智能备份功能， 将数据风险降到最低。 同时具备虚拟机迁移和高可用等技术提高可用性。

5） 弹性扩展

配合 XXX 专利技术 DRX 可以实现资源的弹性扩展， 满足应用的突发需求。

6） 一键部署

提供了虚拟机蓝本及虚拟机和应用的组合操作， 完成一键部署。

13.3.3 云硬盘服务

13.3.4 云存储服务

13.3.4.1 云存储概述

云存储提供对象存储服务。 客户可以通过客户端 / 浏览器访问。 云存储将网络中各类存储设备通过应用软件集合起来协同工作， 对外提供数据存储和业务访问功能的一个系统。

云存储的核心是将数据通路（数据读或写） 和控制通路（元数据） 分离， 并且基于对象存储设备构建存储系统， 每个对象存储设备具有一定的智能， 能够自动管理其上的数据分布。 兼顾对象存储同兼具 SAN 高速直接访问磁盘特点及 NAS 的分布式共享特点。

云存储分为对象、 对象存储设备、 元数据服务器、 对象存储系统的客户端 （或者浏览器） 这几部分。 云存储服务是在云中的、 可无缝扩容的、 高可靠而廉价的存储服务。 它能让您不用关心底层的存储技术， 也不用关心存储资源扩容问题，直接通过对象存储调用海量的存储资源， 为您的应用存储数据。

云存储还提供了快照服务。 快照用于在块设备级别上进行基于时间点的硬盘备份与恢复， 可以同时对多张硬盘做快照（包括系统盘和数据盘） 。 一张硬盘可以有多个快照， 可以随时从任意一个备份点恢复数据。

13.3.4.2 云存储特性

对象存储具有很多先进的特性：

建立在分布式架构之上， 可用性大于等于 99.9%，数据持久性大于等于 99.99999999%

根据系统实际情况， 方案可灵活支撑系统扩容。 扩容包括 3 方面： 流数据扩容、 元数据扩容、 业务系统扩容； 无文件数量限制：

支持部署 MySql 数据库， 单库容量达 1 TB

支持部署 Hbase ， 单表存储空间达 1 OOTB

支持文档、 视频、 音频、 图片等类型的对象存储。 文件大小可达 5TB

通过分布式存储技术实现三份副本， 单台服务器故障不会导致数据丢失。

13.3.4.3 云存储接口 API

云存储提供完整的 API 接口， 帮助与第 3 方系统整合。 提供的是标准的 RestFul 类型接口，同时提供 Java、 Python、 Object-c 二次开发包。

RESTful API 是一个本地接口， 具备最低延迟和最快的响应时间， 。 RESTfulAPI 又名 RESTful Web 服务。 它是一种直观且易用的面向资源的模型， 为大多数 Web 2.0 应用提供服务。 云存储提供的 API 接口如下：

创建文件夹

访问地址： {version}/fileops/create_folder

13.3.5 云数据库服务

13.3.5.1 云数据库服务介绍

基于按需即供的设计思路， 向云应用提供关系型数据库服务， 包括 MySQ、LMS SQL Server、ORACL 等 E 。 功能上支持数据库的创建和访问， 数据库的管理、备份和恢复， 支持用户使用客户端软件进行数据库管理。

云数据库服务设计具有以下产品功能：

1 ） 服务基于高效的调度系统， 备份系统， HA 控制系统， 监控系统；

2） 服务可随着用户数和访问量的变化， 可以灵活地调整数据库的规格， 包含内存、 连接数、

存储容量等；

3） 服务提供 99.95%的高可用性（提供有效服务时间与总时间之比）， 每份数据都保留两份并可实时切换；

4） 服务平台数据库自身的管理和维护， 用户可专注于其的业务功能。

13.3.5.2 云数据库服务使用流程

云数据库服务便捷易用， 一键搞定 ； 多维度监控， 全方位保证安全 ； 性能卓越， 专业团队承诺。

云数据库服务使用主要涉及以下流程：

服务申请

服务使用

服务管理

服务监控

云数据库服务申请：

登录云服务平台， 在资源模块选择数据库服务， 进入数据库服务管理视图。

进入创建数据库入口， 录入用户需求数据库的相应规格参数， 提交申请云平台管理员审批用户资源申请， 触发云数据库服务交付云数据库管理平台控制面板管理所有订购信息通过云数据库服务平台管理视图， 可以查看申请实例的明细信息。

云数据库服务使用：

选择已申请的数据库实例， 查看数据库服务实例配置信息登录云服务器， 在云服务器上使用下面标准 MYSQ 语 L 据库的帐号默认为 root ） 。

句登录云数据库 （云数

mysql -h [云数据库 IP] -P [云数据库端口号] - uroot -p[云数据库密码]

或者使用 MYSQL 客户端使用 IP 和 PORT 登录使用云数据库服务管理

云数据库支持在线无缝升级， 数据库访问不间断 ， 可灵活扩容。

云数据库服务管理支持在线启停实例

云数据库服务管理支持随时退订业务， 保证用户的利益最大化。

此外云数据库服务扩展工具还支持但不限于以下功能自动备份

从备份文件创建临时实例

从备份文件恢复到实例

数据导入导出工具

API 接口

SDK 开发包

文档说明

数据库操作日志管理

数据库管理

账户管理

云数据库服务安全性

支持 IP 授权访问， 通过指定特定 IP 访问提高访问客户端的合法性， 降低受攻击风险。

提供数据库数据存储加密保护， 系统采用数据项级存储加密， 即数据库中不同的记录、 每条记录的不同字段都采用不同的密钥加密， 并辅以校验措施， 以保证数据库数据存储的保密性和完整性， 防止数据的非授权访问和修改。

提供用户加密身份验证， 通过数据库权限控制提供不同的访问权限控制。云数据库服务监控

通过平台监控功能实现对实例级别在不同时间粒度完成对磁盘空间、 连接数、 CPU、 内存、 网络流量等参数的监控数据展示

13.3.5.3 云数据库服务技术架构

云数据库服务交付基于 CSA+OO+（SA 如下图所示） 真正实现全过程的标准化、自动化。 云数据库服务的交付将 Cloud+Automation 技术 密结合， 为用户真正 提供高效和切实的云数据库资源交付使用。

13.3.5.4 云服务自动化平台

云服务自动化平台是云服务中间人， 所有异构云服务的统一管理。

通过云管理平台， 用户从一个门户访问所有云服务 -- 购买 cloud services 、管理 cloud services 。管理员使用单一工具管理所有云服务，将多个云环境的云服务发布到一个单一的目录，管理云上的设备。

云服务自动化平台是开放的， 灵活的， 可扩展的体系结构。

流程自动化引擎

流程自动化引擎是工作流驱动的可扩展性和灵活的可视化 IT 流程自动化平台。 其提供如下技术实现：

提高流程质量

创建可预测和可重复的自动化过程

降低运营成本

自动化手动， 重复和容易出错的任务， 使 IT 人员可以专注于战略计划调整

协调变更

降低了人工交接的低效， 复杂和风险性

提高服务质量

通过自动化的事件和事件分流， 降低升级和诊断和解决平均修复时间 （ MTTR）

平台云允许通过编排你的传统和云基础架构流程以降低成本

提高业务灵活性

可以通过减少时间更迅速地响应不断变化的业务需求来部署新的基础设施和终端到终端的业务服务

可审计的流程

可以记录和执行 ITIL 兼容的， 标准化的流程

便于工作流的创建

允许通过减少需要的专门研发资源， 以减少管理复杂性

自动化实现平台

简单的部署的虚拟设备快速实现价值

统一的物理和虚拟管理

截至最新的合规性报告使治理降低到分钟级别

规模的 IT 自动化通过在多个站点管理数千台服务器

通过整合工具简化操作

基于此技术平台， 按需供应 HA 数据库实例。

MS SQL 高可用数据库服务：

主动模式对数据库服务器进行群集后会有两台虚拟数据库服务器， 如果群集中的某一个节点出现故作， MSCS 控制故障转移， 这使另一个正常的节点需要承受两个节点的服务。

图表 1MYSQ 高 L 可用数据库服务

LVS+Keepalived+MySQL 单点写入主主同步的高可用方案主要实现遇如下问题时， 服务器之间自动切换：

网络问题；

MySQL 问题；

服务器宕机；

Keepalived 服务停止；

13.3.5.5 技术优势

13.3.5.6 数据库性能

目 前支持最高 IOPS 值超过 1 ***0 ， 根据租户不同的业务需求， 选择合适的性能规格的云数据库服务。

13.3.6 云防火墙服务

13.3.6.1 技术特性

对于 XX 市智慧园区大数据云， 需要通过多种形式对外提供云资源的出租服务，在考虑智慧园区大数据云整体安全防护的同时， 也要关注针对不同租户个性化的安全防护需求， 租户的个性化安全部署可以作为云安全服务出租给用户， 在满足用户需求的前提下， 也要达到可运维、 可管理的目的。 XXX 深入分析多租户云安全防护的需求， 提供了两种模式的 vFW 服务可供选择。

通过高性能防火墙实现 IaaS 模型下 vFW 需求

从运维、成本、扩展性的角度考虑，典型的部署模式为通过一台实体或裸机的物理墙进行 1 ：N 的虚拟化， 将不同的虚拟墙提供给不同的租户， 对于租户来讲， 就好像拥有了一台独立的具备一定处理能力的实体物理防火墙， 租户有独立的管理账号， 可以在独立的管理界面， 创建个性化的业务防护策略。 同时作为一种可运营的资源， 类似虚拟机一样， 要求能够给虚墙进行资源分配，逻辑的资源包括接口、 VLAN， 物理的资源包括 CPU、 内存、 存储介质等。 虚墙之间要求数据隔离，并且在共享硬件能力的基础上实现所分配能力的保障， 也即不同虚墙之间不会出现相互侵占的问题， 从而能够实现不同的租户的差异化 SLA 保证。

租户对防火墙申请成功后， 会独享这个 vFW 的资源， 并且具备自己独立配置、管理所租用 vFW 的权利。

通过分布式软件防火墙网关实现 IaaS 下的 vFW

随着云计算虚拟化技术的发展， 越来越多的云计算服务商开始采取 虚 拟 化的网络安全解决方案来满足云租户的安全需求。 云计算服务商往往有非常丰富的服务器计算资源， 而软件虚拟化安全网关的出现也为租户自行运维管理云中的安全服务提供了技术支撑， 典型的部署模型就是 VPC 模型。 云服务提供商给租户提供虚拟机出租， 云租户可以通过在云中部署虚拟化安全网关如 vFW，实现和政府远程分支的 VPN 互联， 使得远程分支用户可以直接访问云中的服务器资源。 通过这种方式政府可以把租用的计算资源作为政府私有云数据中心或者作为政府自有私有云数据中心的有效补充实现混合云， 实现业务需求和成本的有效平衡。

本项目中，软件 vFW 部署 XXX 的 vFW1000 产品，vFW1000 支持多种虚拟平台，基于专业的 XXX Comware V7 平台， 能够监控和保护虚拟环境的安全， 以避免虚拟化环境与外部网络遭受内外部威胁的侵害， 从而为虚拟化数据中心和云计算网络带来全面的安全防护， 帮助政府构建完善的数据中心和云计算网络安全解决方案。

13.3.6.2 安全策略

云防火墙服务是提供给租户在申请云主机、 云存储等服务时配套提供的安全防护服务， 所以

云防火墙的安全策略定义也要与租户的云服务行为相一致， 主要包括外部用户对智慧园区大数据云内部资源的访问控制和智慧园区大数据云内部租户/ 服务器间的访问控制：

外部用户对智慧园区大数据云资源的访问控制策略

基于租户的安全控制要求 ， 配置对内的安全访问控制策略， 实现租户通过政务外网、 公有云、 互联网等对智慧园区大数据云内部资源的可控访问提供租户通过安全 VPN 通道访问智慧园区大数据云内部资源的接入网关， 对接入用户的身份和权限进行认证

提供外部用户访问智慧园区大数据云资源的流量监控和应用层过滤，有效保证智慧园区大数据云基础资源的安全性配置 NAT/NAT Server 策略， 实现对智慧园区大数据云资源访问的内外部地址转换， 并把智慧园区大数据云的对外服务发布到公网上去

智慧园区大数据云内部租户 / 服务器间的访问控制策略

提供安全策略， 保证智慧园区大数据云内部租户、 主机、 VM 之间的默认安全隔离对智慧园区大数据云内部租户主机 /VM 间的互访提供可控的安全访问控制策略

对内部资源共享区， 配置限制访问 / 单向访问控制策略

安全控制策略能够随着租户虚机的迁移而同步， 保证针对同一资源访问策略的一致性

13.3.6.3 技术优势

XXX 在 XX 智慧园区大数据云项目中提供的云防火墙服务具备如下优势：

具备 1 OOG 级别云 FW 服务能力， 根据用户需求可以实现性能平滑扩展

云 FW 设备支持高可靠性部署方式， 实现毫秒级的 HA 双机热备的切换能力

租户可以登录自服务平台并提交云 FW 的需求， 在需求审批通过后， 云管理平台将实现为该租户快速申请 vFW 并实现“分钟级别” 的自动化部署

系统支持多达 1 0 种以上的云 FW 服务模板， 客户在登录云自助服务门户时， 可以结合自身的需求灵活选择各种云 FW 服务模板， 简化了申请的流程

云 FW 服务模板支持用户自定义能力： 客户可以对 FW 的关键指标如吞吐量， 并发连接数目，每秒新建数目及安全策略数目等进行定义

多租户的云 FW 完全隔离， 每个租户的云防火墙服务有独立的配置文件和转发表项， 管理平台将针对不同租户发送独立的安全攻击报告， 保证了多租户之间的数据安全

虚墙能够单独开启、 关闭、 重启， 而不影响其他虚墙业务处理能够在线调整虚墙的处理能力，比如在业务不中断情况下调整虚墙的 CPU 能力占比、 内存占比

每个租户云防火墙具备完整的 FW 功能， 能够支持状态检测防火墙和 VPN， NAT， 攻击防范等功能， 各个云防火墙具备独立管理的能力

13.3.7 云负载均衡服务

13.3.7.1 技术特性

随着 WEB 应用的快速发展和业务量的不断提高， 基于 HTTP/HTTPS 的数据访问流量正在迅速增长， 对政府各行业数据中心以及门户网站等的访问甚至达到了 1 0Gb/s 的级别； 同时， 服务器网站借助 HTTP、 FTP、 SMTP 等应用程序， 为访问者提供了越来越丰富的内容和信息， 服务器逐渐被数据淹没； 另外， 大部分网站（尤其电子商务等网站） 都需要提供不间断 24 小时服务， 任何服务中断或通信中的关键数据丢失都会造成直接的商业损失。 所有这些都对应用服务提出了高性能和高可靠性的需求。

但是， 相对于网络技术的发展， 服务器处理速度和内存访问速度的增长却远远低于网络带宽和应用服务的增长，网络带宽增长的同时带来的用户数量的增长，也使得服务器资源消耗严重，因而服务器成为了网络瓶颈。 传统的单机模式，也往往成为网络故障点。 在这种情况下负载均衡技术应运而生， 负载均衡可以实现对网络设备和服务器带宽的有效扩展， 充分利用多台服务器的业务处理能力，通过合理的调度算法和健康检查双方， 可以有效感知服务器的负载并将业务流量调度到最恰当的服务器上， 从而提高网络的灵活性和可用性。

在 XX 市智慧园区大数据云项目中， 部署了支持 IaaS 架构的云负载均衡设备 L5000-C， 能够为每个租户提供提供独立的 vLB 功能， 实现租户业务的安全隔离，vLB 资源独享也能够保证租户负载均衡服务的性能。

同时， XXX 的云 LB 解决方案能够支持针对虚机的负载均衡， 满足智慧园区大数据云虚拟化云网络资源负载均衡的需要。

用户在申请云服务时，可以根据需求在业务申请界面上选择申请云 LB 服务,在申请云 LB 时，可以根据自身需要， 配置 vLB 的指标参数， 如 vLB 数量、吞吐量、 服务 IP 地址等， 满足用户 vDC 自定义的需求。

租户申请完负载均衡服务后，会有申请流程提交到管理员处，管理在评估用户的业务需求、费用等信息后， 批准 / 驳回用户的云负载均衡服务的申请。

13.3.7.2 负载均衡策略

租户在申请云负载均衡服务时， 可以根据自己业务系统的需要， 合理定义负载均衡策略：

吞吐量： 1 OOM~2G 的吞吐量可自由定义， 满足业务系统和计费需求

设置前端虚服务地址和后端实服务器地址， 实服务动态添加和删除

针对选定的虚服务， 可以选择不同的业务类型： 包括协议类型和端口， 例如 http 协议， 端口 80； 包括 HTTP、 IP 、 TCP 和 UDP 等类型

选择不同的均衡方式： 主要有： 轮转算法， 最小连接算法， 源地址 hash 算法， 目的地址 hash 算法

设置会话保持方式： 会话保持方式包括源地址方法、 源地址端口方法、 目的地址方法、 目的地址端口方法、 源地址目的地址方法等

设置健康检查算法： 支持设定以下健康检查算法， ICMP-echo、UDP-echo、 TCP、 FTP、 SNM、P DNS、 HTTP、 ARP、 IMAP、 POP3 、Radius 、 RTSP、 SIP、 SMTP 、 SSL 等

13.3.7.3 技术优势

快速部署：

租户可以登录自服务平台并提交云负载均衡的服务申请， 在申请审批通过后， 云管理平台将自动快速下发配置并完成服务交付。

服务自定义：

每个租户可以结合自身的业务需求， 选择不同的云负载均衡服务模板， 系统默认支持多种服务模板， 简化租户的服务提交申请流程。

多租户隔离

每个租户申请的 vLB 服务在 CPU、 内存等硬件资源上实现独立保证， 并且每个租户仅能配置自己申请的 vLB， 无法查看和管理其他租户的 vLB， 实现了多租户的安全隔离。

轻量级部署

支持 VMware ESXi、 Linux KVM、 XXX CAS 等多个主流的虚拟平台， 充分发挥虚拟化的优势，实现快速部署、 批量部署、 镜像备份、 快速恢复， 并且能够灵活迁移。

领先的专业平台架构

业界领先的 Comware V7 平台， 支持丰富的网络和安全功能， 能够满足数据中心多租户环境中的应用交付需求。

控制平面和数据平面分离， 专门为虚拟环境优化的多核数据转发， 更能充分利用计算资源。

模块化的体系架构， 开放的网络平台， 允许网络按需运行和控制， 更容易实现 NFV/SDN 落地。

和物理网络设备采用统一的软件平台， 提供相同的功能特性和一致的管理界面。

13.3.8 云入侵防御服务

13.3.8.1 技术特性

当前， 针对各类应用系统的安全漏洞的攻击也一直没有停止过。 在这些应用系统访问的过程中。

目前 Internet 面临的安全威胁从方法上有如下几种：

漏洞利用， 比如针对软件操作系统对内存操作的缺陷， 采用缓冲区溢出方法， 以获得高操作权限运行攻击代码； 如著名的微软 MS05-047 WindowsUMPNPMGR wsprintfW 栈溢出漏洞；

欺骗攻击， 如 IP 地址欺骗等， 其利用 TCP/IP 协议建立的连接未进行认证的缺陷进行源 IP 地址的伪造， 从而达到访问关键信息的目的；

蠕虫 / 病毒， 蠕虫 / 病毒是目前网络上最为常见的威胁， 其具有传播快覆盖广的特点， 如红色代码病毒 (Code Red)， 在 1 2 小时之内覆盖全部的 Internet 网络， 给全球带来了极大的危害； 通常蠕虫 / 病毒通过利用现有系统软件的一些漏洞， 从而达到传播的目的；

木马， 通常在系统中会秘密打开一个访问程序， 以绕过系统的安全策略，从而达到获取信息的目的；

拒绝服务， 通常称之为 DoS/DDoS 攻击， 其通过单台或者多台设备作为攻击的发起者， 对一个特定的目 标进行 DoS 攻击， 从而达到破坏的目 的， 通常拒绝服务攻击会伴随者采用 IP 地址欺骗等方法以隐藏攻击者的目的；

因此部署专业的高性能入侵防御系统实现各类威胁防范显得尤为必要。 智慧园区大数据云的租户可以为其关键应用服务器的流量引入到入侵防护系统进行攻击防护。

通过高性能硬件网关实现 IaaS 模型下 vIPS 需求

从运维、成本、扩展性的角度考虑，典型的部署模式为通过一台实体或裸机的物理墙进行 1 ：N 的虚拟化， 将不同的虚拟墙提供给不同的租户， 对于租户来讲， 就好像拥有了一台独立的具备一定处理能力的实体物理 IPS， 租户有独立的管理账号， 可以在独立的管理界面， 创建个性化的业务防护策略。 同时作为一种可运营的资源， 类似虚拟机一样， 要求能够给虚拟 IPS 进行资源分配， 逻辑的资源包括接口、 VLAN， 物理的资源包括 CPU、 内存、 存储介质等。 虚拟 IPS 之间要求数据隔离， 并且在共享硬件能力的基础上实现所分配能力的保障， 也即不同虚墙之间不会出现相互侵占的问题， 从而能够实现不同的租户的差异化 SLA 保证。 本次项目选用 XXXM9000 上内置的 IPS 模块来实现 IPS 能力， 即保证了与防火墙一致的高性能、 高可靠， 同时也降低了成本。

在 XX 市智慧园区大数据云项目中， 部署云入侵防御服务， 采用 M9000 集成的 IPS 功能， 作为云安全服务提供给租户， 提供入侵防御 / 检测、 病毒过滤和带宽管理等功能。

在租户没有申请入侵防御服务时， 租户的流量不会被送到 M9000IPS 模块进

行安全防护。 对申请了入侵防御服务的租户， 管理员添加流量牵引配置， 把租户的流量引入到 M9000IPS 模块进行安全检测和病毒过滤， 检测通过的流量再向智慧园区大数据云转发。

13.3.8.2 入侵防御策略

云入侵防御服务是提供给租户在申请云主机、 云存储等服务时配套提供的安全防护服务， 与云防火墙一样， 安全策略定义也要与租户的云服务行为相一致，主要为外部用户对智慧园区大数据

云内部资源的安全威胁防御：

基于租户的安全威胁防护要求 ， 配置对内的入侵防御策略， 实现租户通过政务外网、 公有云、 互联网等对智慧园区大数据云内部资源的风险过滤；

提供外部用户访问智慧园区大数据云资源的风险过滤， 有效保证智慧园区大数据云基础资源的安全性

13.3.8.3 技术优势

快速部署：

租户可以登录自服务平台并提交云负载均衡的服务申请， 在申请审批通过后， 云管理平台将自动快速下发配置并完成服务交付。

服务自定义：

每个租户可以结合自身的业务需求， 选择不同的云负载均衡服务模板， 系统默认支持多种服务模板， 简化租户的服务提交申请流程。

多租户隔离

每个租户申请的 vLB 服务在 CPU、 内存等硬件资源上实现独立保证， 并且每个租户仅能配置自己申请的 vLB， 无法查看和管理其他租户的 vLB， 实现了多租户的安全隔离。

轻量级部署

支持 VMware ESXi、 Linux KVM、 XXX CAS 等多个主流的虚拟平台， 充分发挥虚拟化的优势，实现快速部署、 批量部署、 镜像备份、 快速恢复， 并且能够灵活迁移。

领先的专业平台架构

XXX 入侵防护系统在国内服务多年， 积累了丰富的经验， 产品在工行数据中心总行等重要单位得到有效的部署和验证， 作为国内领先的入侵防御产品， XXX 的入侵防护系统具备以下特点：

IPS 模块集成漏洞库、 专业病毒库与应用协议库， 配合 XXXFIRST（ Full Inspection with Rigorous State Test ， 基于精确状态的全面检测） 专有引擎技术， 能精确识别并实时防范各种网络攻击和滥用行为。

IPS 模块集成卡巴斯基防病毒引擎和病毒库。 采用第二代启发式代码分析、 iChecker 实时监控和独特的脚本病毒拦截等多种最尖端的反病毒技术， 能实时查杀各种文件型、 网络型和混合型病毒； 并采用新一代虚拟脱壳和行为判断技术， 准确查杀各种变种病毒、 未知病毒。

XXX 专业安全团队密切跟踪全球知名安全组织和厂商发布的安全漏洞公告， 通过准确的分析，快速生成保护操作系统、 应用系统以及数据库漏洞的特征库

IPS 模块具有强大的攻击防护和流量模型自学习能力， 当攻击发生、 或者短时间内大规模爆发的病毒导致网络流量激增时，能自动发现并阻断攻击和异常流量，以保护路由器、交换机、VoIP 系统、 DNS 服务器等网络基础设施免遭各种恶意攻击， 保证关键业务的通畅。

13.3.9 云 WEB 防护服务

13.3.9.1 WEB 应用安全防护需求

近年来针对网站的攻击不仅仅攻击数量在上升， 种类也在急剧增加， 受攻击范围也在逐步增大， 据统计 95%以上的 Web 站点， 均被黑客“光顾” 过。 Web 网站作为政府和用户、 合作伙伴及员工的快速、 高效的交流平台， 因需要被公众访问而暴露于因特网上， 因此更容易成为黑客或恶意程序的攻击目标， 造成数据损失， 网站被篡改或其他安全威胁。 当前面临的主要 WEB 应用安全问题包括以下几类：

频繁多变的 WEB 应用攻击

Web 应用程序最常见、 最危险的十大安全问题， 包括非法注入、 失效的访问控制、 失效的账户和线程管理、 跨站脚本攻击、 缓冲区溢出、 注射攻击、 异常错误处理、 不安全的存储、 拒绝服务攻击、不安全的配置管理等威胁。 Web 应用攻击与其他网络层攻击不同， 因为它们通常更难被发现， 而且可能来自任何在线用户， 甚至是经过验证的用户。

网页被篡改或被挂马

据国家计算机网络应急技术处理协调中心（简称 CNCERT/C）C 监测， 中国大陆被篡改网站总数逐年增多， 其中， 政府网站被篡改数量也越来越多。 网页篡改事件的屡屡发生， 不仅会给政府的公信力和形象造成不良影响， 也会给人民群众带去不安定的因素。 另外一种篡改方式是网页挂马： 网页内容表面上没有任何异常， 却可能被偷偷的挂上了木马程序。 网页挂马虽然未必会给网站带来直接损害， 但却会给浏览网站的用户带来损失。

数据泄露和被篡改

很多网站数据库中存放着大量的个人敏感信息， 是政府的核心 IT 资产， 但近年来网站数据泄露事件愈演愈烈。 例如社保网站， 个人社保信息一旦泄露将会严重干扰参保人的日常生活， 损害参保人的利益， 甚至制造诈骗等事件等。 同样， 后台核心数据库信息如果被恶意篡改也常常会造成重要的经济损失。

现阶段的安全解决方案通常把重点放在网络层， 当应用层被攻击时， 由于 Web 应用系统的复杂性和多样性导致系统漏洞层出不穷、 防不胜防， 传统的网络层安全设备， 如防火墙， 很容易被 WEB 应用攻击绕过， 难以阻挡此类攻击， 由此需要一系列专门的 WEB 应用防护系统。

通过对 Web 应用系统的安全威胁进行针对性研究， 各种专业的 WEB 应用安全防护技术也应运而生， 以满足全方位的 WEB 网站安全防护要求， 主要包括 Web 应用防火墙、 网页防篡改、 数据库防护技术等。

下面针对各项产品关键技术分别进行介绍。

Web 应用防火墙（ Web Application Firewall, 简称： WAF ） 代表了一类新兴的信息安全技术， 用以解决诸如防火墙一类传统设备束手无策的 Web 应用安全问题。 与传统防火墙不同， WAF

工作在应用层，因此对 Web 应用防护具有先天的技术优势。 WAF 会对所有 Web 流量（包括客户端请求流量和服务器返回的数据流量） 进行深度内容检测和验证， 确保其安全性与合法性， 对非法的请求予以实时阻断， 从而对各类网站站点进行有效防护。

13.3.9.2 WEB 应用安全防护技术

基于规则的检测保护

面对复杂的攻击， XXX WEB 应用防火墙（ WA） F 支持基于规则的保护， 支持丰富的规则特征库， 并能够根据最新威胁实时更新。 针对各种渗透攻击行为， 用户开启这些规则对应用进行全方面检测， 例如 SQL 注入、 命令注入、 cookie 注入、 跨站脚本、 敏感信息泄露、 恶意代码等安全策略， 用于阻断来自互联网的渗透攻击行为。

WAF 提供双向报文检测， 输入检测模块对 WEB 用户提交的 Http 请求协议头、 请求内容进行细粒度解析， 可分类解析 URL、 cookie 、Method、 Request body 等字段， 解析完成后对报文内容进行匹配特征库， 当匹配 SQL 注入、 跨站脚本攻击、 命令注入攻击等特征后， 对报文采用阻断、 放行、 仅检测、 重定向等动作。 WAF 输出检测模块对服务器的响应协议头、 页面内容进行解析， 解析完成后对报文内容进行匹配特征库， 当匹配目录遍录、 错误信息、 信息泄露等特征后， WAF 对报文采用阻断、 放行、 仅检测、 重定向等动作。

基于异常的保护

前面提到的基于规则检测技术是通过特征库匹配技术实现安全防护，需要提取已有攻击特征后才能防护。 但为了应对更为专业复杂的攻击， WAF 会对网站的正常访问行为规律进行分析及总结，建立合法应用数据模型， 并以此为依据判断应用数据的是否存在异常， 当发现不符合该合法模型的行为产生后， WAF 会对该行文进行阻断或告警，以实现对 WEB 应用的防护。 这种方式不需要匹配多条规则特征库， 有助于提高检测效率及准确率。

WEB 业务自动侦测技术

WEB 业务自动侦测技术可对经过 WAF 的流量自动学习， 从混杂流量中学习 WEB 业务服务器信息， 从中获取 WEB 服务器 IP 、 TCP 端口、 域名等信息， 对需要防护的 WEB 应用服务器按需添加至 WAF 的防护中， 从而避免人工配置容易出错， 并节省实施成本。

高性能检测技术

XXX WAF 设备能提供高性能检测能力。 当用户访问时， WAF 会检查其访问的文件类型， 发现访问文件类型为图片、 CSS、 txt 等静态文件时， WAF 直接通过高性能检测模块进行线速转发， 而文件类型为 asp、jsp 或 php 等动态文件则需要规则检测模块进行深度过滤后再转发。 网站访问流量一般为“二八原则” ， 动态文件流量为 20%， 静态文件流量为 80%， 由于 WAF 对静态文件不实行规则检查， 但对存在攻击风险的文件格式仍进行规则检查， 因此既可保证攻击防护有效性，同时又提升了用户访问效率；考虑到安全性，WAF 可仅对常见的静态文件格式进行高性能转发，而对未知的文件类型仍采取规则检测。

同时， XXX 的云 WEB 防护解决方案能够支持针对虚机的 WEB 防护，满足智慧园区大数据云虚拟化云网络资源负载均衡的需要。

用户在申请云服务时， 可以根据需求在业务申请界面上选择申请云 WEB 防护服务：

在申请云 WEB 防护服务时， 可以根据自身需要， 配置云 WEB 防护资源的指标参数， 如云 WEB 防护资源的域名、 服务 IP 地址等， 满足用户 vDC 自定义的需求。

租户申请完 WEB 防护服务后， 会有申请流程提交到管理员处， 管理在评估用户的业务需求、费用等信息后， 批准 / 驳回用户的云 WEB 防护服务的申请。

13.3.9.3 WEB 防护策略

云 WEB 防护服务是提供给租户在申请云主机、 云存储等服务时配套提供的安全防护服务， 与云防火墙一样， 安全策略定义也要与租户的云服务行为相一致， 主要为外部用户对智慧园区大数据云内部资源的安全威胁防御， 租户在申请 WEB 防护服务时， 可以根据自己业务系统的需要， 合理定义需要防护的站点。

基于租户的安全威胁防护要求 ， 配置对内的入侵防御策略， 实现租户通过政务外网、 公有云、 互联网等对智慧园区大数据云内部资源的风险过滤；

提供外部用户访问智慧园区大数据云资源的风险过滤， 有效保证智慧园区大数据云基础资源的安全性。

13.3.9.4 技术优势

快速部署：

租户可以登录自服务平台并提交云 WEB 防护的服务申请， 在申请审批通过后， 云管理平台将自动快速下发配置并完成服务交付。

服务自定义：

每个租户可以结合自身的业务需求， 选择不同的 WEB 防护服务模板， 系统默认支持多种服务模板， 简化租户的服务提交申请流程。

轻量级部署

支持 VMware ESXi、 Linux KVM、 XXX CAS 等多个主流的虚拟平台， 充分发挥虚拟化的优势，实现快速部署、 批量部署、 镜像备份、 快速恢复， 并且能够灵活迁移。

领先的专业平台架构

双引擎架构

设备采用双引擎架构及 CPU 多核绑定技术， 实现流量快速转发， 兼顾 WEB 应用检测的复杂运算， 有效提高防护性能及准确性：

用户行为异常检测引擎， 快速识别正常行为， 提供最优访问体验。

透明代理引擎实现 HTTP 协议完整还原， 从根源上避免绕过及穿透攻击。

专利级检测算法

多项专利技术保障识别能力， 精确识别 OWAST Pop 1 0 等各种 web 通用攻击；

独创行为状态 检测技术， 有效应对盗 、 跨站请求伪造等 WEB 特殊攻击；

国内最为全面的内容管理系统（ CMS ） Oday 防护策略；

独创的访问集中度和 HTTP 协议细粒度检测算法 ， 有效应对了应用层 CC 攻击对业务的冲击。

细粒度控制策略

基于 IP 信用度的动态阻断策略， 对高信用 IP 仅阻断带攻击的请求， 对低信用度 IP 实现网络封锁；

基于 URL 粒度的安全规则实现 WEB 资源的差异化防护；

基于完整 HTTP 协议框架， 可灵活定制各种复杂 WEB 防护特定策略。

纵深业务安全防御

有效应对商业爬虫对商业数据的抓取行为；

有效应对同行发起的恶意预定及抢购行为。

部署灵活运维简单

灵活多变的部署模式， 适应各种网络环境；

站点资源自动发现， 真正即插即用；

策略自学习， 自动生成最符合您业务的专属策略；

日志自挖掘， 展现您最需关注的威胁；

规则库实时更新， 有效应对新型 WEB 攻击。

13.3.10 云防病毒服务

云防病毒服务系统主要由安全控制中心、 查杀服务器（ SVM） 及虚拟机的无代理安全防护组件构成.

13.3.10.1 防病毒管理

虚拟化防病毒采用了云查杀技术， 进行病毒的安全防御。

云查杀引擎， 是完全基于大数据和云计算技术， 不仅扫描速度比传统杀毒引擎快 1 0 倍以上，而且不再需要频繁升级病毒 / 木马库。 只要终端能够连接云 （私有 / 公有） ， 就能实时与云安全数据中心无缝对接，利用服务器端的最新木马库对虚拟机进行扫描和查杀。 因此哪怕是最新爆发的木马或病毒，也能在几分钟内捕获并具备查杀能力，而且占用系统资源极小。实现了用户“零负担” ， 这不是简单的技术创新， 而是安全软件告别“特征库升级时代” 的技术革命。

13.3.10.1.1 云查杀检测引擎

云查杀技术的必要性

随着病毒的大量出现，传统的本地病毒库的查杀方式已经无法在本地加载绝大多数病毒样本特征，目前已发现的病毒样本已经远远超过 20 亿的规模，而目前大多数的终端杀毒软件，受本地存储资源的限制，本地病毒特征库的规模大约在 1 000 万～***0 万左右，这个数字只占不到 20+亿已发现病毒样本的 1%，依靠 1%的病毒库去检测互联网中肆虐的病毒，这说明传统的本地病毒库的查杀方式已经无法满足对已知病毒的查杀要求，需要通过云端的海量计算资源与海量存储资源满足对数十亿病毒进行 1 00%查杀的安全需求。

云查杀资源与技术

云查杀技术需要大量的样本资源、计算资源、检测技术资源，如果没有这些资源作支撑，则无法构建高质量的云查杀系统，本质上来说，云查杀系统是一个海量资源系统，这个资源系统中，既包括客户资源，又包括硬件资源与软件算法资源：

样本资源

构建云查杀系统，需要海量的病毒、木马、僵尸网络等恶意代码样本作为资源支撑，否则，所构建的云查杀系统将因为缺乏足够的病毒样本积累而难以保证对于已知病毒和恶意代码的检测率。本方案中，我们采用的云查杀平台，拥有涵盖了近 20 年的所有已知的病毒、木马、蠕虫等恶意代码的样本文件，其所积累的去重之后病毒样本数量已经超过 20 亿。

样本资源的基础是客户资源，没有足够的客户资源作支撑，无法收集足够的病毒样本文件，只有广泛部署了终端系统的情况下，才能在短期内收集足够数量的恶意代码样本文件，奇虎 360 在全国拥有超过 4 亿的终端用户，覆盖了全国终端用户的 95%以上，其中绝大多数已经选择加入了奇虎 360 公司的“云安全计划”，这些遍布全国的海量用户为 360 提供了丰富、及时的病毒样本资源，保证了云查杀系统病毒样本收集的及时、有效。目前平均来说，一个病毒从首次在国内互联网上出现，到被 360 云查杀系统捕获之间，只有不到 1 0 个小时的时间。

计算资源

为了构造有效的云查杀系统，需要大量的计算资源进行支撑，以便对搜集到的样本资源进行深入分析，一般来说，一台标准的服务器（配置为：双路 1 6 核 CPU（Xeon E5-2690，单路 8 核，主频 2.9GHz）、内存 1 6GB（ ECCDDR） 3、硬盘 900GB（ SAS 接口）），每天（24 小时）可处理的样本数量大约在 3000 万个左右，因此，对于标准 1 000 终端的用户来说，若按照每天每台终端提交 1 0 个样本进行深度检测，则大约需要 4 台服务器组成的云查杀系统才能满足查杀需要。

算法资源

构建有效了云查杀环境，除了稳定、及时的样本收集资源与足够数量的硬件计算环境之外，还需要先进的未知病毒及恶意代码的检测算法，这样才能够在收集到病毒与恶意代码样本之后，进

行有效的分析与处理。 因此， 对未知病毒与恶意代码的快速检测能力， 就成了构建有效的云查杀环境的关键。 在本方案中， 所提供的云查杀环境集成了大量先进的真对未知病毒与恶意代码的查杀算法， 这些算法中， 有基于病毒与恶意代码静态样本共性特征的 QVM-II 算法（该算法采

用人工智能与机器学习的方法， 对目前已经积累的 20 多亿病毒样本进行多次切片学习， 抽取出病毒与恶意代码的共性特征， 建立恶意代码的不同族系模型， 该算法在北美、 欧洲的多项恶意代码检测能力测评之中名列第一）， 也有目前主流的动态沙箱深度分析技术， 同时还集成了利用未知漏洞进行病毒与恶意代码传播的基于内存分析的动态漏洞利用攻击分析技术， 最后， 对于非常复杂、 难于分析的可疑文件， 还会采用具有多年病毒分析与对抗经验的专家分析团队进行彻底分析。 以上这些先机的自动化分析技术与方病毒专家团队人工分析的有效结合， 多种手段、 人机结合， 保证了对病毒与恶意代码分析的万无一失。

13.3.10.1.2 人工智能检测引擎

对于病毒和恶意代码的检测， 一直存在着两个技术方向， 一个是依靠病毒特征匹配的静态检测技术， 这种技术的特点是必须依靠已知的病毒特征， 一般静态特征匹配的技术适合对已知病毒、恶意代码的检测。 另外一种是依靠对病毒行为的动态分析技术， 这种技术更适合对未知病毒、 恶意代码的检测。 这两种技术是目前对病毒进行检测的关键技术， 分别实现对已知、 未知的病毒及恶意代码检测。

其中采用特征对病毒进行检测的技术又分为两个方向， 一个是穷举式病毒特征提取， 即针对每个已发现的病毒、 恶意代码样本提取各自的病毒特征， 这种方式的优点是能够准确识别出已提取特征的病毒与恶意代码， 误报率和漏报率都很低。 另一种是针对不同族类的病毒及恶意代码提取出共性的族群特征， 并以此作为检测依据对恶意代码进行检测。 这种方式的优点是不依赖某一个病毒或恶意代码的具体特征， 而是提取某一族群的恶意代码共性特征， 因此， 这种检测方法对于某一病毒与恶意代码族群内的新生病毒具有非常强的检测能力，同时还能对检测出来的病毒与恶意代码进行族系归类。

人工智能检测引擎采用人工智能与机器学习的方法，对目前已经积累的 20 多亿病毒样本进行多次切片学习， 抽取出病毒与恶意代码的共性特征， 建立恶意代码的不同族系模型。

13.3.10.2 虚拟机安全防护

虚拟化资源池中各个虚拟机计算资源相互独立又可以通过虚拟交换机进行网络通信，因此在对虚拟机进行安全防护时， 不仅需要考虑文件安全防护， 而且还需要考虑例如宏病毒、 内存病毒、注册表病毒、 计划任务病毒和驱动类病毒的查杀， 无代理安全防护组件可以与外部查杀服务器形成智能威胁联动， 可以对上述问题进行有效处理。

13.3.10.3 宿主机安全防护

随着新型威胁形态的不断更新， 威胁态势也开始呈现全面化、 智能化等特点， 而宿主机的安全防护一直以来都是虚拟化防护中的空白， 天擎虚拟化安全管理系统将轻型代理部署至宿主机的 Hypervisor 之中， 能够有效防范针对宿主机的攻击行为。

13.3.10.4 安全策略管理

天擎虚拟化安全管理系统创新的管理架构中首次引入了查杀服务器的角色，由于查杀服务器担负起查杀和更新病毒码的任务，一直以来困扰安全管理员的虚拟化无法差时防护的问题便可以迎刃而解， 而且天擎虚拟化安全管理系统可以直接同步虚拟化平台所有树形结构， 且安全策略可以根据不同需求进行统一管理和分发， 可以大大提升管理运维效率。

13.3.11 云安全增值服务

XX 市智慧园区大数据云项目中， 除了为租户提供云防火墙服务和云负载均衡服务外， 还可根据租户具体应用的需求， 选择流量清洗、 入侵防御、 安全日志审计等增值服务。

13.3.11.1 流量清洗

结合各方统计数据可以看出， 现阶段的 DDOS 攻击活动还处在一个高发期，无论是在持续增长的大小、 速度、 持续时间和复杂性上， 都有了比较明显的增长。

一方面， 网络上充斥的各种 DDOS 攻击工具及详细的指导教程， 降低了黑客的攻击门槛， 使得 DDOS 攻击变成了一种简单高效、极易实施的行为；另一方面，大量的缺乏安全措施的终端 PC，游戏服务器， 各种开放的代理服务器， 也为 DDOS 的攻击提供了数量可观的肉鸡， 使得发动攻击成为可能。

XX 市智慧园区大数据云集中了政府各局的众多应用服务系统，极易成为 DDoS 攻击的目标， 对 DDoS 攻击的防护显得尤为重要。

XXX 部署流量清洗方案来进行 DDoS 防护。 具体部署方案如下， 在智慧园区大数据云出口， 部署 D3000 高端流量检测和清洗设备， 旁挂在接入区交换机设备上， 通过分光或者在接入区交换机镜像等方式对智慧园区大数据云流量进行实时监测， 正常情况下流量直接通过交换机转发， 不会被牵引到流量清洗设备上； 当检测发现攻击之后， 自动在接入区交换机上下发引流策略， 进行流量牵引并完成清洗。

针对这种异常流量， 云计算平台需要提供基础的安全防护能力， 推荐的防护模型包括以下几个方面： 网络业务流量监控和分析、 安全基线制定、 安全事件通告、 异常流量过滤、 安全事件

处理报告等。 其业务实现流程如下图所示：

第一步：将智慧园区大数据云互联网出口流量采用分光或者镜像的方式复制到探测设备上，由探测设备对用户的业务流量进行分析。 并根据分析情况， 制定用户的安全基线。

第二步： 由流量清洗管理平台将探测设备对用户流量的分析结果进行汇总和加工， 形成用户流量分析报告。

第三步： 当发生 DDoS 攻击事件， 由探测设备通知业务管理平台。 业务管理平台会生成安全事件任务进行跟踪。 同时利用短信或者 email 的方式通知维护人员。

第四步： 维护人员基于共同制定的安全策略， 通过管理平台下发到防御设备。

将用务流量牵引至由防御设备， 管理平台组成的“流量清洗中心” 。

第五步： 防御设备在对 DDoS 流量进行过滤的同时， 将当前用户的攻击状况信息发送给业务管理平台。 业务管理平台通过对信息的汇总和加工给用户提供攻击状态报表。 让用户能够随时掌握当前业务状况。

第七步： 攻击停止后， 维护人员基于管理平台上记录的攻击状况信息给用户提供安全事件处理报告并将流量清晰的业务情况报表给用户。

在这个过程中， 用户可以采取手动的方式， 发现攻击之后通过手动进行流量牵引到清洗平台完成流量清晰， 也可以预先设定合理的流量模型基线， 一旦实时监测到的流量超过设定的基线模型就自动进行流量牵引策略的发送并完成本次清洗过程。

13.3.11.2 安全日志审计

对 XX 智慧园区大数据云的租户来说， 把大量应用迁入到云环境后， 也要续遵循各自单位的业务系统安全防护守则， 对日常收到的攻击、 威胁等日志信息进行采集和分析。 为了满足用户的这种需求， XXX 在 XX 市智慧园区大数据云服务管理区部署了安全日志审计服务器。

XXX 安全日志审计网关的价值： 对全网海量安全事件和日志的集中收集与统一分析， 兼容异构网络中多厂商的各种设备， 对收集到的信息高度聚合存储及归一化处理， 实时监控全网安全状况， 能根据不同用户需求提供丰富的自动报告，并提供具有说服力的网络安全状况与政策符合性审计报告。 系统自动执行以上收集、 监控、 告警、 报告、 归档等所有任务， 使 IT 及安全管理员脱离繁琐的手工管理工作， 极大提高效率， 能够集中精力用于更有价值的活动， 保障网络安全。

作为一个综合、 高效的安全信息 &事件管理系统， XXX 日志审计设备具备对异构网络中多种设备的日志 / 事件信息收集并集中分析， 提供事件关联， 帮助准确识别网络攻击， 产品的特点如下：

1 ）支持主流厂商网络设备及主机系统：

不仅能够支持 XXX 各种设备类型， 同时可以支持业界主流网络和安全产品， 支持产品类型高达上百种， 其中包括防火墙、 IPS、 IDS、 路由器、 交换机、 交换机、VPN、 路由器、 防火墙、 IDS/IPS 、 内容过滤系统、 防病毒系统、 防间谍软件系统、防垃圾邮件系统和 Windows、 Unix 和

Linux 主机、 数据库等。

2) 提供网络拓扑和威胁的可视化：

可生成整网安全拓扑视图， 管理员能够通过一个界面直观的查看整个网络安全状态与安全相关的事件。

3) 实时监控与关联分析 ：

提供了对安全事件的集中监控， 能够实时显示每台设备的事件详情，包括源地址、 目的地址、规则号、 用户名、 日期时间、 设备类型、 流、协议、 端口、 描述、 事件 ID、 攻击 ID、 病毒名、 URL、 设备名称等。 通过实时事件显示窗口， 能够轻松了解突发事件， 包括事件起因、发生位置、 被攻击设备和端口， 从而快速纠正危险， 保障网络安全。

面对异构网络中海量事件， 关键事件很容易被淹没。 凭借对网络安全领域的深入研究， 针对常见的安全问题， 提供了几十种预定义的关联告警模板－－智能的“专家系统” 。 同时允许用户自定义安全策略，设定关联模板， 过滤重复信息， 帮助用户快速发现真正的安全隐患，做出重点处理， 防止问题发生。

4) 强大的日志管理功能 ：

由于业界没有关于安全事件格式的统一标准， 因此不同厂商、 不同设备提供安全事件的方式及信息格式差异很大。 设备兼容主流厂商日志格式， 并通过多种方式获取设备日志信息， 包括主动收集、 被动接收等。

通过独特的高聚合压缩技术， 在大数据量情况下（如每天几十 GB）仍能够存储几个月 甚至几年的日志信息。 同时还能自动压缩、 加密和保存日志文件到 DAS， NAS 或 SAN 等外部存储系统，避免了重要安全事件的丢失； 为保证数据可靠性， 用户也可以备份所有日志信息到其他设备中。

5) 安全审计分析 ：

通过对历史信息的深入分析和总结， 用户能够最直接的了解攻击行为和活动， 审计追踪违规行为， 同时可为未来网络非法入侵进行严格界定， 从而对网络安全状况做出预测， 并有针对性的实施安全策略。

6) 完善的报告 ：

报告是来帮助评估网络相关事件的有力手段， 提供了基于角色的访问报告功能， 能够满足个人、 部门以及高级管理等各层次的需求。 另外， 法规已经成为政府的关键问题， 其目的是确保更负责任的行为， 必须符合政府制定的规范， 如：公安部等级保护、 萨班斯法案 (SOX)、 HIPAA、GLBA 等。 XXX 日志审计网关能够提供有针对性报告， 帮助用户遵循法规要求。

13.3.12 云备份服务

在云计算环境中， 云备份服务主要分为两类服务， 第一类服务是对用户本地数据备份到云端的数据备份服务； 第二类服务是对用户运行在云平台上业务应用及数据的备份服务。

第一类云备份服务： 这类云备份服务是云服务商为用户提供本地数据备份到云平台上的服务。

当用户本地数据因本次磁盘或者病毒等原因造成数据损坏且无法恢复时， 可以将备份到云端的数据恢复到本地， 从而达到数据恢复的目的。

这样的备份服务， 一般用户通过云服务商提供 app 软件可以自行完成。

第二类云备份服务： 这类云备份服务的备份对象主要是数据、 云主机和云存储。 依据对象的不同， 具体的备份服务也不同。 例如：备份对象为数据的备份服务：

i.

文件备份服务： 通过在云主机中部署数据备份软件， 实现文件数据的备份服务。

ii.

数据库备份服务： 通过在数据库服务器上部署数据库备份软件， 或者通过数据库自带的备份工具实现数据库数据的备份。

备份对象为云主机的备份服务：

1） 通过云主机快照、 克隆等技术实现对云主机的备份

2） 通过复制软件或者存储复制技术实现云主机的备份。

备份对象为云存储的备份服务：

通过存储复制方式实现云存储的备份。

13.3.13 VPC 服务

13.3.13.1 虚拟私有云 (VPC)架构的特点

在智慧园区大数据云中， 需要实现云租户间的安全隔离。 而 VPC 服务简单讲就是虚拟私有数据中心， 就是在公共云平台上， 创建一套类租户自身私有数据中心的环境。 这个环境对于其他租户而言是完全透明不可见的。 即使两个租户在不同的 VPC 中使用了完全相同的 IP 地址， 相互之间也没有任何影响。 VPC 具有以下优势：

1 ）完全符合安全合规性要求：

从当前云计算安全合规性要求中， 明确要求云计算平台需要提供租户间安全隔离功能。

2） 贴切用户实际需求：

A、 增强安全性： 在智慧园区大数据云中， 各个委办局将自身的业务迁移到云计算平台最为关注点的问题就是安全问题， 安全问题涉及“南北向安全” 和“东西向安全” ， 而 xxxVPC 方案从租户层面即实现了南北向安全， 还实现了租户间的东西向安全； 通过 VxLan 技术的引入， 在跨数据中心环境下即实现大二层网络， 又避免广播风暴在多中心间的泛洪， 保证了网络整体的稳定性和安全性。

B、 实现云、网、安全融合： XXX 的 VPC 方案是通过 OpenStack+SDN+Vxlan+安全网关实现， 这样的方案实现了云管理平台、 网络系统和安全系统的高度融合， 在从而即提高了智慧园区大数据云整体自动化交付能力， 又提高了安全性。

C、 实现原有业务平滑迁移： 智慧园区大数据云首先要解决的是用户的存量业务的上云， 而存量业务 IT 环境复杂， 各个委办局在规划时， 并不是统一规划， 所以， 在 IT 基础设施上会存在冲突， 例如，地址重叠问题， 而 XXXVPC 方案可以实现租户间的完全隔离， 实现租户间完全透明（相互间不可见）， 这样就可以完全避免当前各个委办局间的相互影响； 另外从租户内部通过安全服务 可以灵活的实现委办局当前业务系统部署架构和安全架构，从而保证业务的平滑迁移。

D、 高度兼容性： 网络： 通过提供二层 Vxlan 网关和三层 Vxlan 网关， 是从平滑实现与电子政务网现有网络的互联互通性； 数据库：

XXX VPC 方案对当前传统数据库系统提供有效支持（ Mysql 、 Oracle 和 SqlServer ） 。

3） 可管理性：

A、 模块化： XXX VPC 方案是通过相互独立的模块进行高度融合，各个模块之间既可以实现统一管理又可实现独立管理， 这样可以明确管理边界。 并且避免在对一个模块进行维护时， 造成全局影响。 例如：不会因为对智慧园区大数据云安全网关进行升级时， 造成对计算和应用系统产生影响。 友商方面案例： 友商的 VPC 解决方案是通过在计算虚拟化层高度集成 软件防火墙来实现，而且无法从计算虚拟化平台进行剥离， 在进行安全软件升级时， 出现重大 BUG， 造成全网业务中断。 从这个实际案例可以看出， 模块间相互独立性的重要性。

B、 可管理性： XXX VPC 方案各个组成模块实现相互独立性的另外一个优势就是简化运维管理，明确运维管理边界、 安全边界。

C、 可替换性： 在运行过程中， 无论哪个模块出现问题， 都可以进行独立维护和替换。 从而提高了智慧园区大数据云整体的稳定性。

13.3.13.2 虚拟私有云 (VPC)的实现方式

隔离原理

1. 业务核心、 防火墙将基于不同 vPC 用户虚拟出不同的虚拟设备（如 VRF vRouter、 vFW），每个设备用类似 VRF Index 来唯一区分标识某 vPC 用户的业务；

2. 接入区每个 vPC 用户的一个或者多个业务用一个或者多个 VxLAN ID 进行标识区分；

3. 在业务核心将同一个 vPC 用户的 VxLAN ID 的 interface

与其 VRF 绑定， 业务报文在业务核心、 防火墙、 LB 虚拟设备之间传递时将通过同一个 VRF Index 进行区分， 并且一个 VRF 空间内转发；

4. 反之， 不同 vPC 用户采用不同 VRFindex 进行区分、 并在不同 VRF 空间内转发；

5. 管理网存在与所有 VRF 内的主机互通的需求， 需要在管理核心针对每个 vPC 创建 VRF， 在出口将内部 IP 通过 NAT 转化为外部 IP。

云数据中心内的物理网络资源（ 核心交换机、 接入交换机等 ）， 以及通过主机虚拟化软件的 OVS 均可以提供 SDN、 VxLAN 功能， 组成虚拟网络资源池。

不同租户可通过基于 Openstack 的云平台来调度云数据中心内的网络资源池、 计算资源池、

存储资源池以及安全资源池的资源， 组成自己的虚拟网络 (VPC)。

VPC 内的安全防控，通过使用 Service Chain 的方式调用安全资源池的虚拟化安全组件 (NFV) 来实现， 为不同用户提供 2～7 层的安全隔离。 VPC 网络的部署设计。

VPC 网络构造的方式如下：

1. 通过 SDN 控制器分配不同的 VNI 号将不同的租户分配到不同的 VxLAN 网络中， 实现多租户网络之间的隔离；

2. 通过 SDN 控制器生产不同的 NFV 虚拟设备节点， 为不同的租户提供安全防控服务。

在 VPC 内部， 租户的流量定义如下所示：

1. 通过 Openstack 云平台管理 SDN Controller 实现对于 SDNFabric 、 NFV 设备、 vSwitch 的统一控制；

2. SDN Controller 提供服务 功能， 根据租户需求自定义业务流量编排。 通过服务 的方式，业务流量一开始就严格按照控制器的编排顺序， 经过这组抽象业务功能节点， 完成对应业务功能的处理。

13.4 PaaS 层规划设计

13.4.1 PaaS 概述

XX 市智慧园区大数据云平台服务 PaaS 是建立在基础设施服务 IaaS 之上的， 平台用户可以在上面开发、 测试和部署软件的一种平台; 这意味着， 软件的整个生命周期都可以在 PaaS 上完成。 这种服务模式专门面向应用程序的开发人员、 测试人员、 部署人员和应用管理员。

XX 市智慧园区大数据云平台服务 PaaS 支持应用开发角度的资源抽象化。 在建设 PaaS 平台的时候， 将信息系统中的功能纳入到一个集中的 SOA（面向服务的架构） 平台上， 形成可以复用的服务构件。 然后， 在 PaaS 平台上为各政府部门创建各自独立的用户域， 每个用户域可以选取各自不同的软硬件服务平台， 并按照自己独有的业务环境和模式来组织这些服务。 所有的信息化系统可通过 PaaS 平台聚合

成一个有机的整体。 一方面， 各级政府部门可以通过自己的用户域来组织这些服务， 形成满足自身业务需求的复合应用； 另一方面， 政府部门可以从整体出发， 通盘考虑整个组织的需求，并依此决定是否添加新的业务系统， 而不必自行其事， 造成重复建设。 同样， 新添加的业务系统也可以将自己的功能注册到 PaaS 平台上， 供其他需要的政府机关进行调用。

PaaS 层可根据情况实现数据库即服务、 中间件即服务、 工作流引擎服务和数据即服务等。 这一层服务可以根据需要不断完善， 满足用户定制需求和扩展需求。

13.4.2 PaaS 建设内容

XX 市智慧园区大数据云平台服务 PaaS 将传统的中间件， 身份认证， 工作流， 数据交换， 数据分析等上层应用转变成接口统一、 数据标准的架构。 开发人员不必为他们的应用搭建和配置硬件与软件环境，只需编写应用并将它们加载至 PaaS 上。PaaS 平台会负责管理服务器和虚拟层，剩余部分则交由用户管理。 由于 PaaS 中的服务器操作系统和应用开发环境也由专人负责维护， 因此开发人员能够将精力集中在创建应用上， 而不用时刻关注服务器软件升级， 由用户数量增加带来的软硬件性能要求提高等问题。 另外， 由于平台服务 PaaS 会指定开发语言， 部分特殊应用还是会选择 IaaS 服务。

PaaS 平台以搭建主流的开发测试环境及开源的软件开发平台为主， 提供中间件接口服务， 数据交换服务等加快实现各单位业务系统的开发测试及部署。

13.4.3 PaaS 服务

通过搭建 PaaS 平台， 各单位可以充分利用平台所提供的服务接口， 开发设计用户所需的应用系统， 从而将精力和资源都专注到业务流程和程序代码的设计上， 摆脱了维护测试环境和开发工具的烦恼，大大减少了开发难度和工作量，提高了工作效率，降低了应用程序生命周期成本。利用 PaaS 平台开发测试与传统模式的对比：

数据库即服务：

基于按需即供的设计思路， 向云应用提供关系型数据库服务， 包括 MySQ、L MS SQL Server、ORACLE 等。 功能上支持数据库的创建和访问， 数据库的管理、 备份和恢复， 支持用户使用客户端软件进行数据库管理。

数据库即服务设计提供以下功能：

服务基于高效的调度系统， 备份系统， HA 控制系统， 监控系统；服务可随着用户数和访问量的变化， 可以灵活地调整数据库的规格， 包含内存、 连接数、 存储容量等；

服务提供 99.95%的高可用性（提供有效服务时间与总时间之比） ，每份数据都保留两份并可实时切换；

服务平台数据库自身的管理和维护， 用户可专注于其的业务功能。

应用模板即服务：

应用模板服务将可视化托拽各类基础服务制作完整开发测试模板， 包括选择应用所需要的网络安全环境、 虚拟机、 操作系统、 数据库以及中间件等， 打包为一个针对某特定项目开发的 vAPP，能够正常部署、 启动， 并且可以发布到服务.

目录供其他部门或者云平台下的组织使用：

初始化软件上传， 把需要自动化部署的操作系统、 中间件、 应用的基础软件上传云管理平台后续选择。

应用模板创建， 按照用户可按照所需应用要求通过图形化拖拽方式选择所需资源以及所部署的软件等。

应用模板发布， 待模板创建完毕可选择模板发布共其他部门或用户使用。

创建应用实例， 用户可按照需求自行选择相关模板部署为应用， 部署成功后可通过云平台直接查看状态。

13.4.4 PaaS 优势

XX 市智慧园区大数据云平台服务 PaaS 的优点如下：

第一， 集中部署。 建设大型的数据中心， 可以保证高可靠性， 针对用户不同的业务系统， 可以提供不同档次的服务器硬件平台， 并可以根据客户业务系统的发展， 灵活地调整其部署的硬件平台规格。 各级政府部门可以方便地开通或注销某个应用平台， 而无需分别维护各自庞大的硬件和软件体系。

第二， 各取所需。 根据各级政府用户自身的要求， 灵活选取丰富的基础硬件中的功能， 为政府机构构建符合其自身需求的 IT 架构。 由此， 政府部门可以快速定制不同机构的端到端业务流程， 更加贴近各个机构用户自身的业务特色。

第三， 灵活应变。 由于所有的业务系统都作为功能库在 PaaS 平台上得到开放， 当新需求出现或软件需要调整时， 只要将各个服务组件之间的关联关系重新调整一下， 就可以很快地应对变化。

第四， 简化维护。 将原先独立维护、 各自为政的应用作为应用构件， 整合为一个完整的信息架构， 并在真实的业务流程中加以调用， 能大大简化维护负担，提升用户的使用体验。

13.5 云管理平台

13.5.1 云管理平台整体架构

云管理是整个智慧园区大数据云后台的管理、 调度、 运维中心。 基于 Openstack 平台的商业化云服务平台， 在 承原有架构灵活、 扩展性强、 开放性和兼容度高的基础上， 产品稳定性和可靠性大大增强。基于租户到应用的端到端的云服务配置和管理，将用户申请的服务组装成服务 ，统一管理和配置。 通过对租户的分级管理， 实现了私有云多级资源分配的要求， 通过定制个性化的审批流程， 使得服务的申请更符合某些特殊业务的多级审批要求。 通过对服务 的健康状态的整体监控和评分， 对每个租户的总体服务质量有全面的把握和管理。

云管理平台是云业务的管理中心， 可以融合资源池化、 生命周期管理、 业务中间件管理、 租户管理、 身份认证、 安全管理、 计费与账务、 服务运营、 服务水平管理、 业务流程自动化等

内容， 是调度、 管理云资源必不可少的手段， 是云时代 ITSM/BSM 的新的业务形式。

13.5.2 设备管理

13.5.2.1 网络管理

全面的管理设备类型

XXXiMC 智能管理平台实现网络资源、内部用户和业务的融合管理，提供基本的网络资源管理、拓扑管理、 故障管理、 性能管理、 内部用户管理及系统安全管理， 基于 B/S 架构， 可以与 XXX iMC 其他业务组件有效集成， 形成多种解决方案。

XXXiMC 智能管理平台不仅可以实现 XXX 全线数据通信产品的管理， 也可通过标准 MIB 实现对 Cisco 、 华为、 迈普等各主流厂商的数据通信设备管理。

除了传统的路由器、 交换机外， 更能对网络中的无线、 安全、 存储、 语音、监控、 视频、服务器、 虚拟设备、 打印机、 UPS 等设备进行管理， 实现设备资源的集中化管理。

告警管理

告警管理流程

告警管理亦称故障管理， 是 iMC 智能管理平台及其他业务组件统一的告警中心， 为内部用户提供统一的全流程故障管理体系。

通过设备 Trap 上报与主动轮询双向确保快速准确发现网络故障。

通过实时告警关联分析， 屏蔽重复无效告警， 分析生成根因告警。

通过实时告警与拓扑提示、 通过告警板声光提示、 通过手机短信及 Email

等远程提示， 快速通知网络管理员详细准确的故障信息。

通过固化内部用户维护经验， 为后续相关告警处理提供经验参考与快速定位指导。

实时远程告警： 手机短信及 EMail 告警

解决故障

固化经验

分类、 声光告警板， 按故障类别及等级实时告警

实时告警关联

分析与统计

实现网络管理

透明化

网管与告警中心

实时告警

实时告警浏览和确认

系统快照， 实时报告网络、 下级网络及设备的状态

告警上报 定时轮询

通过拓扑实现报告网络及设备状态

网络资源、 存储资源、 计算资源、 业务系统

性能监视

一目了然的网络 TopN 性能指标

CPU 利用率、 内存利用率、 带宽利用率、 设备响应性能、 设备不可达等是网络性能管理中用户最关注的几项， XXX 智能管理中心通过 TopN 列表， 使用户对当前网络中的性能瓶颈能够一目了然。

性能视图

用户可灵活定制性能数据浏览视图， 分析网络运行趋势。 性能视图支持多指标多实例数据组合的展示， 支持 TopN 明细表格、 TopN 柱图、 折线图、 柱状图、面积图、 汇总数据多种性能监控数据展示方式。

性能与告警的深度结合

XXX 智能管理中心支持对每一个性能指标设置两级阈值， 发送不同级别的告警。 用户可以根据告警信息直接了解到设备监视指标的性能情况， 有助于用户随时了解网络的运行状态， 预测流量发展趋势， 合理优化网络。

拓扑管理

丰富、 实用的网络拓扑视图

除传统的 IP 拓扑视图外，XXX 智能管理中心平台还提供全网络的拓扑视图和自定义拓扑视图，使用户可以根据自己的组织结构、 地域情况、 甚至楼层情况清晰灵活地绘制出客户化的网络拓扑。在全网络拓扑视图中， 用户可以随意组织和定制子图。

增强的二层拓扑

传统实现的拓扑都是基于 IP 的三层拓扑，XXX 智能管理中心平台在此基础上更支持二层拓扑，实现了同一个 VLAN 或者网段内部 PC 与网络设备、 二层网络设备之间的互连关系， 更方便直观的体现了网络中设备的互联关系。

嵌入式拓扑

资源自定义视图、 IP 视图中实现设备的列表式管理和拓扑管理的融合。 拓扑中支持添加任意的文字标签， 比如下图的“杭州数据中心” 。

嵌入拓扑使用 HTML5 技术， 不需要安装 Java 插件就能支持。 同时， 在 iPad 、Surface 等移动设备上也能正常显示。

数据中心机房、 机架拓扑

XXX 智能管理中心支持按设备物理位置进行组织的数据中心机房和机架拓扑。通过此拓扑视图，用户可以很方便的找到设备在机房中所处位置， 进而对设备物理实体进行管理维护。

数据中心拓扑： 支持数据中心、 机房、 云图、 路等拓扑对象， 提供全局的数据中心监控。

数据中心楼层 - 机房分布拓扑： 在数据中心内部管理、 监控各机房在各楼层的分布。

流量拓扑

以端口流量和网络负载为主要视角， 向使用者展示所关注的网路拓扑结构和流量负载数据统计及分析情况。

13.5.2.2 安全管理

安全设备管理

实现安全设备的安全域、 IP 、 服务、 规则等配置获取， 实现对单个设备的安全域、 IP 、服务、 规则进行调整和优化。

虚拟设备管理

提供物理设备 -> 引擎组 -> 虚拟设备的树状关系管理， 并可以在拓扑上体现折叠关系。

SSM 监控各个虚拟设备的 CPU/ME，M 依据此调整虚拟防火墙分配的 CPU/MEM 参数。

在“虚拟设备管理” 中增加的所有虚拟设备都将加入到“设备管理” 中， 对于安全业务来说虚拟防火墙和物理防火墙是一样的。

IP 地址管理

在部署规则时可以基于 IP 地址组定义规则。

服务管理

基于用户服务进行域规则组织。

不同服务组合成服务组

设备监控

设备吞吐量监控

在“设备管理” 中监控所有设备的当前 CPU/MEM 利用率， 并发连接数、 新建连接数指标， 点击相应连接可以查看历史数据。

规则有效性监控

业务运行一段事件后， 规则数量会越来越多， 运维人员面对数以千计的规则无从下手， 不知道哪些规则是否还有用处。 SSM 监控每条规则的匹配速率和最后一次匹配时间， 若规则上次匹配命中的时间很久了或速率很低， 则在“规则优化管理” 中提示用户需要调整该规则了。

安全事件分析及日志接收

在“攻击事件明细” 中针对某一个攻击， 安全管理可以在拓扑中绘制出攻击路径， 并可以限制攻击源的连接速率，这样可以有效控制 flood 攻击，或通过 EIA 将其下线。“日志综合审计” 提供统一的查询分析功能， 如某源 IP 都发送什么攻击、 做了什么 NAT 转换、 发生过什么域间访问等信息， 一次性搜索到相关的所有类型的信息。

设备安全日志接收， 支持 NAT 和 Syslog 格式日志， 其中 NAT 方式支持 syslog 格式和二进制格式。

13.5.2.3 服务器管理

XXXFlexServer 系列服务器后端都硬件集成 1 个独立的 GE 管理端口， 也就是 iLO（Integrated Light-Out ） 口。 用 iLO 口可实现对服务器的硬件级别的管理。

iLO ManagementEngine 是一整套嵌入式管理功能， 支持服务器的整个生命周期， 包括最初部署、 日常管理以及服务警报和支持。 iLO 是 iLO ManagementEngine 的一项功能。

iLO 子系统是 XXX FlexServer 服务器的一个标准组件， 它可以简化初始服务器设置、 服务器运行状况监视、 电源和散热优化以及远程服务器管理。 iLO 子系统包括智能微处理器、 安全内存和专用网络接口。 这种设计使 iLO 独立于主机服务器及其操作系统。

iLO 启用和管理 Active Health System ， 还具有 Agentless Management 。

iLO 监视所有重要的内部子系统。 启用 SNMP 警报后， 无论主机操作系统是什么或是否安装了主机操作系统， iLO 均直接发送这些警报。 无论采用什么操作系统软件和服务器上有无安装操作系统代理， 具有 iLO3 的 XXXFlexServer 服务器上均内置远程支持软件。

通过使用 iLO， 可以执行以下操作：

监视服务器运行状况。iLO 监视服务器中的温度并向风扇发送校正信号以维持正常的服务器散热。 iLO 还监视固件版本以及风扇、 内存、 网络、 处理器、 电源和内部存储的状态。

下载 Active Health System 日志、 支持案例未解决时， 可发送日志文件。

如果具有到服务器的网络连接，则可以从世界上的任何地方访问服务器的高性能且安全的集成远程控制台。 集成远程控制台具有两个版本：

.NET IRC

Java IRC

除非另有说明， 否则， 通常所说的远程控制台适用于 .NET IRC 和 JavaIRC。

使用共享 .NET IRC 与最多 4 个服务器管理员进行协作。

将高性能虚拟介质设备远程安装到服务器上。

从 GUI 、 CLI 或 iLO Scripting Toolkit 中使用虚拟电源和虚拟介质执行很多任务， 包括自动部署和配置。

安全地远程控制管理的服务器的电源状态。

监视能耗和服务器电源设置。

通过 iLO 发出 SNMP 警报以实现真正的 Agentless Managemen，t 而无论主机服务器处于何种状态 .

使用本地或基于目录的用户帐户登录到 iLO。

使用 iL O 语言包在汉语和其它支持的语言之间切换。

使用远程管理工具控制 iLO。

13.5.2.4 存储管理

XXX P8*** 作为行业领先的存储产品， 其卓越的阵列管理功能可以消除存储层的复杂性， 从而减轻存储管理的负担。 在提高系统透明度和控制的同时， 还消除了昂贵的、 重复的和易错的手动任务。 以 P8*** InForm 操作系统为依托 ，可提供一系列软件产品来提高用户公用存储部署的敏捷性和高效性

XXX P8***InForm 操作系统

P8*** InForm 操作系统采用先进的内部虚拟化技术， 可提高管理的效率、系统利用率和存储性能。 同时， InForm 操作系统能够在子系统层面对存储配置和变更管理进行智能地自动化处理，且无需管理人员的介入， 从而简化了系统的存储管理。 所有类型的 InServ 服务器都支持 InForm 操作系统， 因此所有 P8***阵列都享有同样的内置软件虚拟化和自动化功能。

P8***InForm 管理控制台

P8***InForm 管理控制台通过一个统一的、 点击式界面， 简化了系统管理。

该界面支持所有 P8***InForm 软件产品， 且为 InServ 阵列内所有的物理和逻辑对象提供非常丰富的指示。 这种丰富的指示， 配之以强大和个性化的报告功能，消除了对更多软件工具的需求，用户也无需因为故障查找和诊断而咨询专业的服务。SNMP 和 SMI-S 可提供开放式的管理支持。

精简技术

P8*** 所提供的软件产品独具特色， 因为采用了业界仅有的 ThinBuiltIn

硬件架构， 精简配置， 削减高达 75%的 SAN 成本、 占地空间和能源开支， 无需为每个应用或服务级别分配存储资， 也无需支付不必要的电力、 空间和磁盘散热费用。

精简转换

利用 ThinBuiltIn 架构， 精简转换可以将全配置的存储简单、快速地转换为精简配置的存储，从而消除多达 75% 的原有容量。

精简持续

精简持续可以回收已删除卷的空间， 从而使您的存储长期保持精简。 该软件可实现主机文件系统与 InServ 的智能通信， 以回收与文件删除相关的容量空间。

数据保护和灾难恢复

P8*** 的数据保护和恢复产品依托硬件独有的、 灵活高效的写入复制快照技术， 后者使用户能够以低成本最大限度地实现恢复点和恢复时间目标。

FullCopy

以独立的服务级别参数创建时间点克隆。 支持快速重新同步化且具备精简配置感知功能。

VirtualCopy

虚拟复制是一款无预留、非重复的写入复制软件产品，可以让您保护和共享任何应用数据。有了虚拟复制， 用户再也无需为存储预留容量，并且变更的数据永远不会在快照树中被复制。

Remote Copy

远程复制可以更为经济地保护和共享任何应用数据。 远程复制凭借精简复制技术， 使中高端阵列融为一体， 还消除了专业服务的需求， 从而大幅降低了远程数据复制和容灾的成本。

多客户端弹性和安全性

P8*** 提供多个具备数据弹性和安全性的产品， 旨在与多客户端公用存储阵列协同工作。

VirtualDomain

虚拟域这款虚拟机软件可为不同的应用和用户群提供安全、独立的访问和强大的存储服务， 以及更高的存储服务级别， 包括性能、 可用性和功能性。

VirtualLock

虚拟锁定能够实现存储卷安全的保留。 在和无预留的、 非重复的快照一起使用时， P8*** 虚拟锁定为数据监管和法律搜索流程提供了高效的存储基石。

自动管理

简单而高效的解决方案具备多项自动策略管理功能，可提供更高的可靠性并减少存储管理时间。

AdaptiveOptimization

自适应优化利用 P8*** 经过验证、 细粒度的数据移动引擎， 可应用于卷内独立的存储区域，从而实现高度可靠的、 连续的自动分层存储， 在合适的时间将合适的服务质量（ QoS） 匹配给合适的数据。 在实现服务级别目标的同时节省高达 30%的存储成本。

DynamicOptimization

在多个存储层上连续的分配和再分配应用卷，以确保应用需求与按需的数据服务质量级别相一致。 分析卷如何使用物理磁盘， 自动进行不间断的智能化调整， 以确保最佳的卷性能和容量利用率。

AutonomicGroups

自动组可创建主机、卷和域的分组，以加快存储配置的自动化。您只需要点击 3 次鼠标和 60 秒时间， 就可以完成多个卷的创建并将其配置到多个虚拟服务器。 快速配置。 快速配置通过较低级别组件的细粒度虚拟化，可提供即时、 应用定制的配置， 从而消除了阵列规划任务。 存储配置管理可智能且自动的进行， 同时内部资源的数据条带化确保可为所有工作负载类型提供可预测的高级别服务。

System Reporter

是一个易于使用、 基于 Web 的性能和容量管理工具，可将一个或多个 InServ 存储服务器的历史系统信息集合在一起。 对于服务级别协议（ SLA） 和 chargeback 支持而言， SystemReporter 是满足其故障排除、 规划、 综合的监测和收集信息需求的理想之选。

Host Explorer

自动进行主机搜索和收集详细的主机配置信息， 以加快配置和简化维护。 可确保主机信息和主机多路径数据到 InServ 的安全通信， 以减少手动管理。

13.5.3 资源管理

登录云管理平台， 在资源模块选择数据库服务， 进入数据库服务管理视图。

通过该视图可以完成日常数据库管理的在线操作。

通过云数据库管理平台可以给用户在数据库管理带来以下好处

1）便捷： 用户可以快速的在云平台中申请实例资源

2）易用： 按需自助在线操作， 无需进行任何的代码改造。

3）安全： 提供在线的主从两份数据存储， 确保线上数据安全。

同时通过备份机制保存多天的备份数据以便于在灾难情况进行数据恢复。

4）高性能： 集中安装专用高性能存储服务器来支持海量访问。

5）省心：提供 7×24 小时的专业服务，扩容和迁移对用户透明且不影响服务。 提供全方位、全天候立体式监控。

管理员登陆 iMC 后台， 看到每个委办局租户申请的主机、 网络、 数据库等资源。

13.5.3.1 IP 资源管理

VLAN 管理

VLAN 管理提供了对设备的 VLAN 规划， VLAN 配置下发等功能。 通过 VLAN 管理对网络的 VLAN 进行统一的规划， 然后把这些配置统一下发到设备上， 完成网络的 VLAN 管理。 同时 VLAN 管理组件还提供 VLAN 拓扑功能， 可以直观的查看到 VLAN 的部署情况。 VLAN 管理的功能包括： 全网 VLAN 管理、 VLAN 设备管理、 VLAN 配置报告、 VLAN 拓扑、 VLAN 批量部署。

ACL 管理

iMCACL 管理定位于网络 ACL 资源管理， 结合交换机和路由器设备， 提供智能化的 ACL 资源管理， 可严格实现客户所需的访问控制策略， 从而实现对网络访问的最终权限控制， 方便管理员对 ACL 进行批量配置， 提高解决方案的易用性， 减轻网络管理人员的工作量； 既可实现对单设备的配置管理， 也可方便内部用户实现对多设备的批量配置管理。

IP 地址管理

随着在数据中心网络中服务器、 PC 机、 打印机、 语音电话等（注： 下文将服务器、 PC 机、打印机、 语音电话等直接称之为网络终端） 网络终端的增加，对这些网络终端的管理难度越来越大， 同时这些网络终端接入网络时的安全认证风险也越来越高。 iMC IP/MAC 终端准入管理提供一套简洁的工具，帮助网络管理员对网络终端的安全接入进行管理和控制。终端准入管理通过 IP 地址分配、终端准入绑定、 交换机准入绑定、 IP-MAC 绑定、 终端异常处理策略和日志记录等方式，实现对网络中终端资源的统一管理与监控。

13.5.3.2 主机应用管理

iMC APM 应用管理是为了帮助智慧园区大数据云各种业务的监控管理需求而提供的应用监控管理解决方案， 它提供了强大的系统与应用监控管理能力， 可以对不同的业务系统、 应用和网络服务 （如服务器、 操作系统、 数据库、 Web 服务、中间件、 邮件、 其他关键应用等） ， 进行远程监控和管理，从而充分满足智慧园区大数据云用户对各种关键业务和数据中心的监控管理需求。

iMC APM 采用易于部署的 Web 架构， 并提供友好的安装向导， 即使是不熟悉相关技术的维护人员， 也可以在半小时内安装完毕， 并初步搭建起对政府各种应用提供监控的管理平台。 iMC APM 同时支持 Agentless （无监控代理） 和 Agent 代理的最新技术， 用户可根据自身需要进行选择适合方案。 APM 提供了自动发现应用、 应用监视、 主机监视、 分类监视、 应用分组等模块， 同时拥有报表功能。

当被监视的应用出现异常时， iMC 应用管理就会产生告警， 通过这些告警， 可以鉴别出问题的根本原因。

全方位监视功能

iMC APM 基于 B/S 架构， 安装过程非常简单， 界面简洁明了， 一般管理人员在短时间内就可以掌握， 降低了部署和使用成本。

iMC APM 可以监视各种应用程序和服务器， 包括应用服务器、 数据库、 操作系统、 邮件服务器、 Web 服务器、 各种服务以及自定义的监视器， 可以为整个业务基础架构提供统一的视图。 APM 还提供监视器分组功能， 可以将相关的设备关联到一个监视器组中， 方便管理。

APM 可根据用户不同需求定制不同应用展现层次：

主机监视： 应用管理从应用所在服务器 /PC 的角度提供了应用监视的功能，可方便地查看到各服务器 /PC 自身和部署应用的运行情况；

概览视图： 概览视图提供了系统监控应用所在主机的列表， 并列出了该主机上监视应用的可用性和健康状况。

列表视图： 列表提供了系统监控应用所在主机的列表， 给出了主机自身的可用性和健康状况，并提供了主机上监视应用的列表。

分类监视： 应用管理从应用类型的角度提供了应用监视的功能， 可方便地查看到各应用类型的汇总分析情况。 分类监视概览提供了系统支持监视的应用类型的列表， 并列出了每个应用类型所包含应用健康状况的汇总数据。

APM 可以对被监视参数设置阈值， 在严重故障发生之前就发现问题， 产生告警， 从而实现主动的监控， 大大提高了服务的可用性。 iMC APM 通过智能事件 -告警关联分析技术， 在产生告警的同时生成根本原因分析， 协助管理人员对故障进行处理， 减少了故障时间。 iMC APM 支持各种标准的通知方式， 如发送电子邮件、 短信、 SNMP TRA、P 记录工单， 也可执行自定义的程序来自行修复故障，使用户不需要坐在电脑前，就可以获得告警信息，从而能够及时地解决问题。APM

用不同的颜色来表示不同重要度的警报， 让管理人员一目 了然， 快速掌握整个业务基础架构的情况。 管理人员还可以对告警添加注释， 为今后的故障处理提供了参考。

查看 APM 告警的详细信息时， 点击告警分类的 接可直接联动到该应用的报告页面。

在应用报告页面， 显示了该应用 Top5 未恢复告警， 并以背景色标识告警的严重级别。

监视报表

iMC APM 为所有的监视器及其重要参数提供了内置报表， 通过报表用户可以查看这些监视对象一段时间内的变化趋势。 iMC APM 可以提供日报表、 周报表、月 报表、 年报表、 自定义时间报表还有排行报表， 报表可以导出为 pdf 、 csv 格式， 打印报表， 也可以通过 E-mail 发送报表。 iMC APM 还提供日程报表， 可以计划需要生成报表的时间， 并发送到指定的邮箱中。

监视融合

iMC APM 与 iMC 智能管理平台实现了完美的融合， 不仅可以从业务的角度进行管理， 也可以从网络的角度直接监控业务。 APM 作为一个组件可以通过 iMC 监控代理进行安装， 并允许用户通过监控代理查看、 启动、 停止 APM 进程。 在 iMC 管理平台的设备详细信息和拓扑图中可以选择被监控的服务器， 直接查看被监控的各种业务系统的运行信息。 也可调用 APM 的应用监控功能，查看进一步的应用名称、 应用类型、 可用性状态和健康状况。

13.5.3.3 服务健康管理

ITIL 要求 IT 服务部门通过服务水平管理来保证其服务有效， 建立服务健康水平监督体系，来保证服务达到规定的健康水平等级， 即使服务失败， 也可以正确分析原因， 帮助 IT 服务部门做出正确的应对决策。

服务健康管理系统（以下简称 SHM） ， 正是定位于 IT 服务的健康监控管理方案， 服务是指数据中心提供的一系列业务， 例如语音服务、 邮箱服务等。 基于 iMC 系统的网络性能、 告警、NQA 路监控， NTA 流量分析、 APM 应用管理等业务模块， 提取关键性能指标（ KPI） ， 建立服务各个方面质量的度量指标（ KQI） 以及服务整体质量的度量模型（ SLA） ， 基于服务可用性、MTTR、MTBF 等的监控和分析对服务的健康水平做出评价。用户可以通过 KQI 的创建与服务的建立，来完成整个服务的度量监控和管理。 通过丰富的图形报表， 可以将关键质量指标直观的展示出来，从而更容易的了解数据中心的整体服务水平并及时发现潜在问题。

13.5.3.4 数据库管理

登录云管理平台， 在资源模块选择数据库服务， 进入数据库服务管理视图。

通过该视图可以完成日常数据库管理的在线操作。

通过云数据库管理平台可以给用户在数据库管理带来以下好处：

1） 便捷： 用户可以快速的在云平台中申请实例资源

2）易用： 按需自助在线操作， 无需进行任何的代码改造。

3）安全： 提供在线的主从两份数据存储， 确保线上数据安全。

同时通过备份机制保存多天的备份数据以便于在灾难情况进行数据恢复。

4）高性能： 集中安装专用高性能存储服务器来支持海量访问。

5）省心： 提供 7×24 小时的专业服务，扩容和迁移对用户透明且不影响服务。 提供全方位、全天候立体式监控。

13.5.4 资源编排

13.5.4.1 网络资源池化

受网络设备硬件和协议的限制， 网络的许多配置是有限制的， 如每个设备上的 ACL 数量受到 ACL 号的限制和硬件的限制， 中低端设备的 ACL 数量不超过 ***0 个、 VLAN 号最多只有 4096 个、网络总带宽受到接口带宽的限制、 不同设备的不同接口支持的 ACL 和 QoS 的能力也是不同的， 等等。 RAM 对网络资源和设备能力进行池化， 为后续的网络编排、 服务匹配及服务模拟部署提供支撑， 是 RAM 自动化的基石。

统一的网络设备适配层

网络设备适配层支持 SNMP/Telnet/SSH/Netconf/Restful/SOAP/WMI/Shell 等各种网络基础架构层的访问方式， 支持对物理设备和虚拟设备的统一管理， 支持对网络资源和计算资源的统一管理， 支持路由器、 交换机、 防火墙、 LB、hypervisor 的统一管理， 支持 XXX、 Cisco 、 Huawei、F5 等多主流网络厂家设备的统一管理。

RAM 的 VLAN、 ACL、 QoS 等是基于 IMC 业务组件实现的， 使得 RAM 快速提供广泛的设备支持能力。

13.5.4.2 网络域和租户管理

网络域是整体网络的一部分， 通常是租户到应用或服务器的端到端网络。 对于某个租户或应用来说， 从租户到应用的端到端网络配置完全可以在一个网络域上完成实施。

可以基于网络域设置租户的接入端口作为接入点， 并将这些接入点与租户绑定。 这里的租户代表使用网络或应用的人。

13.5.4.3 基于业务的可视化服务编排

引入服务单元（ Service Unit ） 的概念， 服务单元是服务编排的最小单位。

网络模型

在业务编排中引入网络模型的概念， 将网络按照层次进行切分， 从而使得网络结构更加清晰。系统提供常用的网络结构模型， 管理员可以根据自己的网络结构创建出自己的网络模型， 甚至定义自己的网络角色。

基于业务的正向编排

在服务模型编排界面， 直接拖拽服务单元构造符合业务拓扑的逻辑拓扑结构。 支持基于服务单元的配置， 不同的服务单元支持不同的配置项。

基于网络域的反向编排

在网络域上选择相关设备后， 能够快速的创建出贴合实际拓扑结构的业务逻辑拓扑， 而不再需要拖拽服务单元构造业务逻辑拓扑。

13.5.4.4 服务快速申请与撤销

基于服务目录的服务模型管理

编排完成的服务模型统一存储在服务目 录中， 提供服务目 录的增删改， 可以为不同的服务模型指定不同的图标， 管理员可以上传自己的图标文件。 服务模型提供掠过式逻辑拓扑展示， 方便用户快速浏览各个服务模型。

服务模型作为一个模板能够重复地应用在不同的网络域， 为不同的租户提供部署服务。 服务模型和网络域必须基于相同的网络模型才能够进行匹配。

智能服务自动匹配

以网络资源池化数据为基础，根据各个设备的支持能力与服务模型中的配置智能的匹配拓扑路径。

智能服务冲突检测

以网络资源池化数据为基础， 对新增的网络配置进行全面检查， 检查的错误主要包括：

与本设备的冲突， 如 VLAN 虚接口 IP 已经被占用；

与整网配置冲突， 如从租户到 VLAN 虚接口没有一条有效的路径， 再如 QoS 带宽保证配置时网络接口带宽不足；

与其他服务的未下发配置冲突 （服务一旦创建， 相关的网络资源都会被预留） 。

可规划的业务部署

创建服务时可以指定服务的执行类型：立即执行或按租期执行。允许指定租期的起至时间，系统将根据租期的开始时间定时部署配置到设备上， 也会根据根据租期的结束时间自动去部署网络配置。 执行部署前可以对配置进一步执行冲突检测， 进一步提高配置下发的有效性。

服务创建后， 可以随时去部署已经部署的服务， 或立即部署未部署的服务。

13.5.4.5 全面的服务监控

资源池监控

提供设备级网络资源池化、 路径资源池化及 LB 设备资源池化。

设备级池化主要包括端口、 ACL、 VLAN 的可用资源等；

路径资源池化主要包括选定两点之间的路径、 端口、 带宽及路数等；

LB 设备资源池化主要包括吞吐量、 连接数、 CPU 和内存利用率、以及当前配置的 virtual server 等。

租户监控

租户监控提供全部租户的 dashboard 和单个租户的 dashboard 。 全部租户 dashboard 提供服务租期统计、 Top5 带宽利用率、 Top5 设备告警、 Top5 阈值告警、 以及租户接收报文速率和发生报文速率； 单个租户 dashboard 提供设备状态统计、 Top5 设备告警、 租户带宽统计和 Top5 带宽利用率等。

13.5.5 资源监控

iMC APM 应用管理是为了帮助智慧园区大数据云各种业务的监控管理需求而提供的应用监控管理解决方案， 它提供了强大的系统与应用监控管理能力， 可以对不同的业务系统、 应用和网络服务 （如服务器、 操作系统、 数据库、 Web 服务、中间件、 邮件、 其他关键应用等） ， 进行远程监控和管理，从而充分满足智慧园区大数据云用户对各种关键业务和数据中心的监控管理需求。

iMC APM 采用易于部署的 Web 架构， 并提供友好的安装向导， 即使是不熟悉相关技术的维护人员， 也可以在半小时内安装完毕， 并初步搭建起对政府各种应用提供监控的管理平台。 iMC APM 同时支持 Agentless （无监控代理） 和 Agent 代理的最新技术， 用户可根据自身需要进行选择适合方案。 APM 提供了自动发现应用、 应用监视、 主机监视、 分类监视、 应用分组等模块， 同时拥有报表功能。

当被监视的应用出现异常时， iMC 应用管理就会产生告警， 通过这些告警， 可以鉴别出问题的根本原因。

全方位监视功能

iMC APM 基于 B/S 架构， 安装过程非常简单， 界面简洁明了， 一般管理人员在短时间内就可以掌握， 降低了部署和使用成本。

iMC APM 可以监视各种应用程序和服务器， 包括应用服务器、 数据库、 操作系统、 邮件服务器、 Web 服务器、 各种服务以及自定义的监视器， 可以为整个业务基础架构提供统一的视图。 APM 还提供监视器分组功能， 可以将相关的设备关联到一个监视器组中， 方便管理。 如下图所示，展示自定义应用的整体性能概览。

APM 可根据用户不同需求定制不同应用展现层次：

主机监视： 应用管理从应用所在服务器 /PC 的角度提供了应用监视的功能，可方便地查看到各服务器 /PC 自身和部署应用的运行情况；

概览视图： 概览视图提供了系统监控应用所在主机的列表， 并列出了该主机上监视应用的可用性和健康状况。

列表视图： 列表提供了系统监控应用所在主机的列表， 给出了主机自身的可用性和健康状况，并提供了主机上监视应用的列表。

分类监视： 应用管理从应用类型的角度提供了应用监视的功能， 可方便地查看到各应用类型的汇总分析情况。 分类监视概览提供了系统支持监视的应用类型的列表， 并列出了每个应用类型所包含应用健康状况的汇总数据。

点击“基层社会管理综合系统” ， 可以展开其中包含的应用类型及状态

点击详细报告， 可展示智慧园区大数据云中详细应用系统的可用性报告：

监视故障根源

APM 可以对被监视参数设置阈值， 在严重故障发生之前就发现问题， 产生告警， 从而实现主动的监控， 大大提高了服务的可用性。 iMC APM 通过智能事件 -告警关联分析技术， 在产生告警的同时生成根本原因分析， 协助管理人员对故障进行处理， 减少了故障时间。 iMC APM 支持各种标准的通知方式， 如发送电子邮件、 短信、 SNMP TRA、P 记录工单， 也可执行自定义的程序来自行修复故障，使用户不需要坐在电脑前，就可以获得告警信息，从而能够及时地解决问题。APM 用不同的颜色来表示不同重要度的警报， 让管理人员一目 了然， 快速掌握整个业务基础架构的情况。 管理人员还可以对告警添加注释， 为今后的故障处理提供了参考。

查看 APM 告警的详细信息时， 点击告警分类的 接可直接联动到该应用的报告页面。

在应用报告页面， 显示了该应用 Top5 未恢复告警， 并以背景色标识告警的严重级别。

监视报表

iMC APM 为所有的监视器及其重要参数提供了内置报表， 通过报表用户可以查看这些监视对象一段时间内的变化趋势。 iMC APM 可以提供日报表、 周报表、月 报表、 年报表、 自定义时间报表还有排行报表， 报表可以导出为 pdf 、 csv 格式， 打印报表， 也可以通过 E-mail 发送报表。iMC APM 还提供日程报表， 可以计划需要生成报表的时间， 并发送到指定的邮箱中。

监视融合

iMC APM 与 iMC 智能管理平台实现了完美的融合， 不仅可以从业务的角度进行管理， 也可以从网络的角度直接监控业务。 APM 作为一个组件可以通过 iMC 监控代理进行安装， 并允许用户通过监控代理查看、 启动、 停止 APM 进程。 在 iMC 管理平台的设备详细信息和拓扑图中可以选择被监控的服务器， 直接查看被监控的各种业务系统的运行信息。 也可调用 APM 的应用监控功能，查看进一步的应用名称、 应用类型、 可用性状态和健康状况。

展示了智慧园区大数据云中 “基层社会管理综合信息系统” 的应用拓扑关系。

服务健康管理

ITIL 要求 IT 服务部门通过服务水平管理来保证其服务有效， 建立服务健康水平监督体系，

来保证服务达到规定的健康水平等级， 即使服务失败， 也可以正确分析原因， 帮助 IT 服务部门做出正确的应对决策。

服务健康管理系统（以下简称 SHM） ， 正是定位于 IT 服务的健康监控管理方案， 服务是指数据中心提供的一系列业务， 例如语音服务、 邮箱服务等。 基于 iMC 系统的网络性能、 告警、 NQA 路监控， NTA 流量分析、 APM 应用管理等业务模块， 提取关键性能指标（ KPI） ， 建立服务各个方面质量的度量指标（ KQI） 以及服务整体质量的度量模型（ SLA） ， 基于服务可用性、MTTR、MTBF 等的监控和分析对服务的健康水平做出评价。用户可以通过 KQI 的创建与服务的建立，来完成整个服务的度量监控和管理。 通过丰富的图形报表， 可以将关键质量指标直观的展示出来，从而更容易的了解数据中心的整体服务水平并及时发现潜在问题。

13.5.6 用户管理

13.5.6.1 用户管理策略

iMC 用户是系统及各业务组件的管理维护人员， 不同的操作员拥有不同的管理权限。 此外还可以通过操作员访问控制列表来限制操作员访问系统时所在的位置；通过密码控制策略来控制操作员的密码复杂度及密码失效后的处理方式， 并且任何操作员都可以修改自己的密码； 通过在线操作员管理来管理正在执行系统维护工作的所有操作员；通过操作日志来审计和跟踪操作员执行的操作。 操作员闲置超时时长为登录后的操作员提供更进一步的保护， 当登录后的操作员闲置时间超过操作员闲置超时时长时， 系统自动将操作员注销。 在操作员登录时， 系统还提供了另一个角度的安全保护： 连续三次登录不成功的操作员， 系统会在一段时间内禁止其登录， 以避免恶意登录尝试。

13.5.6.2 用户权限控制

通过权限管理， 可为不同的 iMC 操作人员规划不同的权限， 从而实现精细化分权管理能力。

iMC 智能管理平台提供多维度精细化权限管理， 分别为： 基于业务功能维度（操作员分组） 和数据资源维度。 iMC 提供这两个维度的交叉权限管理能力。

对业务功能维度通过操作员分组来划分， iMC 可以控制特定业务具体功能的可用性， 例如修改用户基本信息等。

系统缺省存在管理员、 维护员和查看员三个缺省分组， 也可以在此基础上创建新的分组， 类似角色概念， 进行更为精细化的权限控制。

对数据资源维度，iMC 通过设备分组和可分级的用户分组，配置操作员可访问的数据资源。当操作员用户特定用户分组管理权限时， 只能看到此分组下的用户。 无权访问的业务功能和数据资源对操作员均不可见。

13.5.7 流程管理

市政府局委办、 市政府办公厅电子政务处、 电子智慧园区大数据云服务商群组拥有各级审批权限。 租户发起申请后， 首先对应的局委办会在流程中看到一条审批申请， 他可以点击完成审批。 审批后， 市政府办公厅电子政务处在流程中会看到一条审批申请， 他可以点击完成审批。 最后流程走到云服务商， 审批通过， 可以启动资源创建， 并通知租户资源分配完成， 租户获得云资源。

上述流程的定制后台， 即依赖于 iMC SOM 来实现。 SOM 是面向 IT 运维服务的管理解决方案，关注 ITIL 服务生命周期中关键的服务转换和服务运营部分，聚焦于和 IT 基础架构管理关系 密的运维流程的支持能力。 SOM 通过流程化管理能力， 使所有的 IT 运维活动（比如配置的变更、 故障问题的处理） 做到可控、可度量、 可审计。

13.5.7.1 智慧园区大数据云开通流程

13.5.7.2 实时精确的联合 CMDB

CMDB 是 IT 运维服务管理的核心部件， 和一般的资产管理相比， 除了资产配置项本身信息，还维护各配置项之间的关系、 当前状态和变更情况。 iMC SOMCMDB 采取“ CMDB 核心数据” 加“原始业务资产数据” 的管理组织方式， 通过联合的 CMD，B 可以帮助内部用户度量系统 IT 资产的价值， 为服务管理流程提供有关 IT 基础设施的准确信息， 为故障管理、 问题管理、 变更管理和发布管理等的运作提供后台支持。

13.5.7.3 完整的服务运维流程

iMCSOM 组件从关注服务运维流程的角度出发， 提供了配置管理、 变更管理、请求 / 事件/ 故障管理、 问题管理等 IT 网络运维流程的全生命周期管理。

13.5.7.4 故障维护流程

iMC SOM 的网络故障维护流程， 实现了与 iMC 故障告警功能的融合， 为内部用户提供了一个从定位、 审核、 修复到确认关闭的闭环过程， 保障网络故障得到及时有效处理。

13.5.7.5 变更流程

iMC SOM 的网络配置变更维护流程可以和 iMC 配置管理相融合， 使 IT 管理人员通过 iMC 所

做的所有网络变更操作都满足受控、 可审计的要求， 提高内部用户对网管操作的透明度和信任度。

13.5.7.6 流程定制

不同的内部用户对实际运维流程有各自习惯和强制要求， 为了适应这种差异，iMC SOM 组件提供了从流程各个步骤到流程模板的灵活定制能力。 内部用户可以基于系统预置的流程模板， 定义适用的流程。 在流程定义中， 可以指定流程的优先级、 各阶段任务的可操作内部用户。 对于高级内部用户， 可以使用脚本语言创建或定制流程模板。

13.5.7.7 知识库管理

iMC SOM 集中的知识库保存解决方案避免了重复工作， 并通过有效的知识共享，提高了整体生产效率， 不管是哪个技术人员处理请求， 内部用户都能得到一致的回答。

13.5.7.8 服务台

iMC SOM 组件的服务台功能为运维人员提供了个性化的工作空间， 为所有运维活动提供了理想的工作平台。

在每个运维人员的工作区中， 提供了和个人相关的运维工作内容。 配置管理、变更管理、 请求 / 事件/ 故障、 问题管理、 知识库管理等所有运维活动， 也都可以在这个服务台上衔接完成。

13.5.8 日志管理

13.5.8.1 操作日志管理

iMC 能够记录所有相关管理员在 CSM 云平台的相关活动的日志， 并对其进行审计。 操作日志用于显示和查询操作员在执行管理任务中的一些关键操作的基本信息， 例如操作员登录系统、 对设备进行添加、 删除和配置等操作的基本信息。

日志管理包括查看详细信息、 查询等操作。 其中查询可以按照操作员、 IP 地址、模块名称、操作结果、 开始时间、 结束时间和操作描述进行查询。 另外， 管理员可以通过数据转储功能对操作日志进行备份和删除。 如果日志量过大， 系统提供了操作日志的自动转储功能， 满足转储条件的操作日志会被系统备份成文件后存储到指定目录下， 并把转储的数据从系统中删除。

13.5.8.2 SYSLog 日志管理

Syslog 日志接收

XXX 智能管理系统支持多厂商设备的 SYSLOG 原始报文接收， 提供日志浏览、查询、 导出及自动转储功能。

Syslog 日志提取与分析

XXX 智能管理系统支持在海量日志中提取重要信息， 并升级为告警， 及时提示内部用户关注。

支持按日志类别、 日志级别分析提取；

支持统计分析提取， 如在 300 秒内连续收到 50 次日志“ VTYlogin ”， 则产生告警提示内部用户。

支持生成告警级别及描述设置。

内部用户可按需设置生成告警的级别， 也可以设置告警描述。 如可配置生成“ VTYlogin flood ” 告警； 可配置成“ %SYSLOG ” %告警， 即将 SYSLOG 日志原文直接做为告警描述提示给内部用户； 也可配置成“ Duplicate address$(Duplicate IP) on $(Source VLAN) ” 告警， 即通过提取 SYSLOG 中关键参数信息组成告警描述提示给内部用户。

支持解析模板定义， 对 SYSLOG 日志原文进行分析提取。

模板内容可以直接输入不带参数的匹配文本， 如： “ -IP address IPcollision detected ” 。匹配文本可以输入“ *” 通配符， 代表一个或者多个字符。 模板内容支持匹配文本中带有参数，参数的形式： $(参数名称)， 如：

“Duplicate address $(Duplicate IP) on $(Source VLAN)” ， 系统会自动提取参数信息供后续分析及告警生成使用。

13.5.9 报表管理

XXXiMC 智能分析报表解决方案基于 B/S 架构， 将报表分析和报表展示能力与 iMC 无缝集成，实现从数据提取、 数据转换和数据展示等功能， 提供有效报表系统解决方案。

开放数据源

iMC 开放的数据源是自定义报表的基础， 涵盖了 iMC 预定义报表使用的几乎所有数据源， 对于自定义报表开发来讲是完备的。 iMC 平台开放的是基础网管的数据， 包括资源、 性能、 告警模块， 每个业务组件也会根据自己的设计开放完备的数据源。

ETL 分析能力

iMC 报表平台同时内嵌的 ETL 模块（数据提取、 转换、 加载） ， 提供强大的智能分析能力，作为有力的数据分析工具， 在 iMC 开放的原始数据源和对应复杂报表需求的内部用户自定义报表数据源之间搭建起了一个桥梁。

预定义报表模板

iMC 平台和各业务组件提供了丰富的预定义报表模板， 对于大部分内部用户， 已经完全能够满足日常的报表需求。

报表设计功能

业界领先的报表设计器（ iAR)， 提供可视化的自动义报表设计环境。

设计环境用户操作融合

iMC 报表平台提供 iMC 数据源配置的导出功能，简化了报表设计过程中的数据源建立过程。而对于内部用户来讲， 数据库连接和数据源的建立往往是最不容易完成的操作。 从而使报表设计工作轻松上手。 iMC 目前支持 Oracle 、 SqlServer 两种数据库， 并使用 JDBC 来连接数据库， 导出的数据源配置就是这两种数据库的 JDBC 连接。

很多时候， 内部用户只是对已有报表的部分细节不满意； 这时可以将 iMC 中的预定义报表直接导出为报表设计工程文件， 在报表设计器中进行调整后， 再导回到 iMC 报表平台中使用。 如下， 选择 RPT 格式即可导出报表设计工程文件。

使用报表设计器设计出来的自定义报表模板的发布操作非常简单，只需要在报表平台上执行一个增加操作， 即可将新的自定义报表模板等同于原有的预定义模板使用。

在报表平台中， 可以使用报表模板创建各类周期的报表， 包括天报表、 周报表、 月 报表、季度报表、 半年报表、 年报表。 可以设定周期性报表的开始时间、失效时间。

完成一次性配置后， 就可以自动化的产生周期性的报表结果。

对所有的报表模板， 都可以使用立即报表的操作查看实时的报表数据， 而不必等到每个周期结束时。 有助于实时的发现定位问题。

报表分发

对于自动化生成的周期性报表， 可以根据需要发送给不同角色的内部用户，比如决策人、 投资人、 管理员等。 如果采用手工的操作， 将是一件繁重的工作，iMC 报表方案提供了自动化的 Email 发放报表方式。

13.5.10 计费策略管理

针对智慧园区大数据云到租户， 以及租户到内部终端用户的分级计费统计，针对服务类型和服务时间提供灵活的计费方式。 两个策略可以不同。

计费策略自定义， 基于云服务（ 主机、 存储、 数据库、 应用 ）对资产进行数据采集、 计量、 预处理， 提供账单、 结算报表。

计费策略可以定制结算周期， 最小计费单位等。 整个私有云有一个基本使用费用（类似月 租费） ， 然后加上各个资源申请使用的单个计费。 各个计费资源，例如 CPU， 也有初始基本费用和后续递增费用。

市政务专有云基础资源服务 IaaS 提供给用户计算、 存储、 网络， 安全和其它基本资源。 局委办用户通过 IaaS 服务能够部署和运行其应用系统。用户不需要管理或控制任何云计算基础设施

硬件， 但能选择操作系统、 储存空间、 部署的应用， 也可控制防火墙和负载均衡器。 客户可以基于这些服务进行编排， 构建属于自己的虚拟数据中心。

13.6 云安全体系

13.6.1 云平台安全建设要求

智慧园区大数据云安全的需求实际上就是要合理地解决智慧园区大数据云信息安全与信息共享、开放性之间的矛盾。 在智慧园区大数据云系统保证安全性和机密性的基础上， 保持信息共享和通讯畅通的效率。 然而随着信息技术的发展，Web2.0、 SOA 和云计算技术的涌现， IT 的信息安全一直没有良好的保证。 对于智慧园区大数据云， 摆在我们面前的威胁有着多种。 移动设备、 远程设备连接、 浏览器以及各种应用程序的插件程序、 智能终端、 云主机的出现， 都为信息安全带来了新的挑战， 而内部攻击者和系统漏洞仍然为信息安全最大威胁。

智慧园区大数据云所涵盖的信息系统是政府机构用于执行政府职能的信息系统。政府机构从事的行业性质跟国家 密联系， 所涉及的众多信息对安全性要求都比较高。 一方面， 政务信息关系到党政部门、 乃至整个国家的利益， 比个人或商务信息更为敏感， 需要更高的安全性； 另一方面， 智慧园区大数据云行使政府职能的特点导致更容易受到来自外部或内部的攻击， 包括黑客组织， 犯罪集团和信息战时期的信息对抗等国家行为的攻击。

综上所述， 智慧园区大数据云的安全总体需求可分解为如下内容：

(1) 保护政务信息资源价值不受侵犯；

(2) 保证信息资产的拥有者面临最小的风险和获取最大的安全利益；

(3) 保证政务的信息基础设施、 信息应用服务和信息内容为抵御各种安全威胁而具有保密性、完整性、 真实性、 可用性和可控性的能力。

13.6.2 智慧园区大数据云平台安全标准要求

(1) 公安部云计算等级保护安全技术要求：

如果云平台同时承载二级等保信息系统和三级等保信息系统， 则要求云计算平台必须通过等级保护三级等保要求， 并且有如下安全要求：

①二级等保信息系统和三级等保信息系统的计算资源要物理隔离。

②二级等保信息系统和三级等保信息系统的存储资源要物理隔离。

(2) 国标： 信息系统安全等级保护 - 云计算安全要求云平台合规性要求：

安全合规：提供安全可靠的云平台，为政府服务的智慧园区大数据云其安全性更高的要求；业务系统三级等级， 需要支撑平台通过相应的等级保护认证。

规范运维： 完善云平台安全体系和管理制度， 以便提升整体安全管理水平，规范应用系统开

发商和运维商的行为， 确保承载的系统和数据的安全稳定。

(3) 云安全标准

①中央网信办发《关于加强党政部门云计算服务网络安全管理的意见》 ；

②国家公安部发《信息系统安全等级保护基本要求云计算安全技术要求》 、《信息系统安全等级保护测评要求云计算要求》 ；

③国家信息中心发《智慧园区大数据云安全技术要求与实施指南》 、《智慧园区大数据云平台安全等级保护测评方法与规范》 。

13.6.3 等级保护重点要求及分解应对措施等保内容 应对措施

1 、 网络安全 / 结构安全

a) 应实现不同租户之间虚拟网络资源的隔离 ， 并避免网络资源的过量占用;

通过 VxLAN 技术为每个租户分配虚拟网络， 利用 NFV 技术为租户分配独立的边界安全控制资源， 结合 VRF、 QoS 技术可确保网络层隔离与带宽保障

b) 应绘制与当前运行情况相符的虚拟网络拓扑结构图， 并能对虚拟网络资源、 网络拓扑及相应访问控制策略进行实时更新和集中监控云平台支持

c) 应根据租户各部门的工作职能、系统业务类型、 重要性和所涉及信息的重要程度等因素 ，为虚拟机划分不同的安全区域

d) 应保证虚拟机只能接收到目的地址包括自己地址的报文 ；

e) 应保证业务网、 存储网、 管理网组网架构分离 ；

f) 应能识别、 监控所有虚拟机之间、宿主机与虚拟机之间的流量 ；

g) 应提供开放接口 ， 允许接入第三方安全产品。

三方安全产品可通过 Openstack 框架接入服务 支持第三方安全设备通过代理网关接入

2、 网络安全 / 访问控制

a) 在虚拟网络边界应部署访问控制设备, 启用访问控制功能 ；

通过 VxLAN 隔离租户网络， 利用 NFV 技术在虚拟网络边界部署 VFW 进行访问控制

b) 应采取安全的技术手段避免直接通过互联网管理云资源 ；

管理网与业务网隔离， 管理中心边界部署防火墙进行访问控制

c) 应依据安全策略启用虚拟机间的访问控制功能。

通过 NFV + 服务 技术在租户虚拟数据中 心 内 部部署 VFW 实现虚拟机间访问控制

3、 网络安全 / 安全审计

a) 应为安全审计数据的汇集提供接口 ， 允许可信的第三方接入 ， 实现集部署安管平台实现集中审计等保内容 应对措施中审计。

4、 网络安全 / 入侵防范

a）应能够检测租户通过虚拟机访问宿主机资源 ，并进行告警 ；

b）应能检测到租户对外的攻击行为，并能记录攻击类型、 攻击时间、

攻击流量 ;络出口部署 NGFW 实现双向流量的攻击检测

c）应具备对异常流量和对未知威胁的识别、 监控和防护能力 ；

通过 NFV + VxLAN 技术在租户虚拟网络出口部署 NGFW 实现双向流量的监控

d）应对有害信息发布等安全事件进行实时监测和告警。

通过 NFV + VxLAN 技术在租户虚拟网络出口部署 NGFW 实现双向流量的内容监控与审计

5、 网络安全 / 网络设备防护

a）应采取安全可信的方式对管理用户进行接入认证 ；

b）应实现租户和云服务商管理用户的权限分离 ；

c）应在网络控制器和网络设备 （ 或设备代理 ）之间建立双向身份验证机制;

需 VCFC 支持(目前还不支持 VCFC 与设备间的双向身份验证，理论上承载 netconf 的 HTTPS 协议和下发流表的等保内容 应对措施

OpenFlow 协议均可以提供双向身份验证机制)

d）应保证网络安全策略只能通过云平台进行统一配置和发布 ；

管理网与业务网隔离， 管理网边界部署防火墙进行访问控制， 仅允许管理终端登录云平台进行管理操作

e）应采取必要措施防止网络控制器和网络设备 （ 或设备代理 ）之间的网络通信被窃听和嗅探。

6、 主机安全 / 身份鉴别 b）应建立安全可信的接入认证方式，保证管理用户对虚拟资源访问的安全性。

c）云平台 web 接口不应使用自签名证书。

采购权威的签名证书

7、 主机安全 / 访问控制

a）应保证云服务对物理资源的调度和管理均在资源抽象层内完成 ，应隔离平台内承载信息资源的云服务对平台物理资源的直接访问 ；

b）应启动访问控制功能 ，依据安全策略控制虚拟机间的访问 ；

c）应采取安全控制措施 ，防止通过虚拟机漏洞获得对所在物理机的访问和控制 ；

d）应采用技术措施保证不同虚拟化实例之间的资源隔离 ；

e）应确保逻辑卷同一时刻只能被一个虚拟机挂载 ；

f）应采用安全措施保障数据库实例隔离;

g）应采用安全措施防止云服务商非授权访问云租户数据或者利用租户信息进行数据分析。

h）应实现租户管理用户和云服务商管理用户的权限分离 ；

8、 主机安全 / 安全审计

a）审计内容应包括重要用户行为、虚拟机间迁移、 虚拟资源调度、 虚拟资源分配、 虚拟资

源的异常使用和重要系统命令的使用等系统内重要的安全相关事件 ；

c）应保证云服务商对租户系统和数据的操作可被租户审计。

9、 主机安全 / 剩余信息保护

a）应采取技术措施在虚拟资源回收时，对数据进行清除。

b）应确保云用户在退出时 ， 数据多个同上冗余得到清除。

1 0、 主机安全 / 入侵防范

a）应能检测到未经授权打开的端口，并提供告警 ；

b）应能够检测云用户通过虚拟机访 CAS + CVM 提供保障等保内容 应对措施

c）应确保虚拟资源在启用后 ， 供用户使用时 ， 版本或补丁保持最新 ；

1 1 、 主机安全 / 恶意代码防范

a）应确保虚拟资源在启用后 ， 供用户使用时 ， 及时进行恶意代码软件版本和恶意代码库升级 ， 并进行恶意代码检测 ；

b）应能够检测恶意代码感染及在虚拟机间蔓延的情况 ， 并提出告警。

1 2、 主机安全 / 虚拟机安全

a）应提供虚拟机自动迁移功能 ， 支持虚拟机实例从其他物理机启动 ；

b）不同虚拟机之间的虚拟 CPU 指令隔离 ；

c）虚拟机不能迁移至低于其所在系统安全等级的环境 ；

d）应提供自动保护功能 ， 当故障发生时自动保护当前所有状态 ， 保证系统能够进行恢复 ；

e）应屏蔽虚拟资源故障 ， 某个虚拟 CVM 保障等保内容 应对措施

f）应对物理资源和虚拟资源按照策略做统一管理调度与分配 ；

g）应禁用虚拟内存优化技术 ， 保证虚拟内存的独占访问 ；

h）应保证虚拟资源的业务处理能力具备冗余空间 ， 满足业务高峰期需要;

i）应限制单个虚拟机对物理资源的最大或最小使用限度 ；

j）当对同一台物理机上有多个虚拟机进行漏洞扫描与恶意代码防范时 ，应将漏洞扫描与恶意代码防范产品部署在对资源的消耗控制在安全的范围内。

k）应按照对业务服务的重要次序来指定虚拟资源分配优先级别 ， 保证在资源 张的时候优先保护重要业务服务所占用资源 ；

l）监控信息的汇集提供接口 ， 允许 部署安管平台实现集中审计等保内容 应对措施可信的第三方接入 ， 实现集中监控 ；

1 3、 主机安全 / 镜像和快照保护

a）应提供虚拟机镜像文件完整性校验功能 ， 防止虚拟机镜像被恶意篡改;

b）应采取加密或其他技术手段 ， 防止虚拟机快照中可能存在的敏感资源被非法访问 ；

1 4、 主机安全 / 资源监控

a）当监测到应用服务过载时 ， 应能够根据预设的策略自动扩展计算资源，确保应用服务质量 ；

1 5、 主机安全 / 安全开发

a) 应采用安全技术措施 ， 保障资源访问的应用编程接口安全。

对编程接口开发进行安全规划， 对发布的编程接口进行安全测试

1 6、 主机安全及备份 / 数据安全

a) 应确保在虚拟资源迁移过程中 ,虚拟资源数据的完整性 ， 并在检测到完整性错误时采取必要的恢复措施。

b) 应确保在虚拟资源迁移过程中 ， 云计算平台资源调度时需要规划设计等保内容 应对措施

虚拟资源数据的保密性 ， 防止在虚拟

a) 租户应对业务数据进行定期备份。

从管理层面对租户落实备份制度云平台支持存储、 数据库资源的分区

b) 对于重要数据存储的位置应限定在安全可控的地理范围内 ；

c) 应提供虚拟资源的数据级冗余备份机制。

a) 租户与云服务商服务合约到期时 ,应完整地返还租户信息。

b) 在租户定义的时间内 ， 清除云服务平台上存储的租户信息 ， 并确保不能采用技术手段恢复。

c) 云服务商应协助租户将信息迁移到其他云服务平台或者传统的 IT 平台。

1 7、 管理及人员安全

a) 云服务商对云租户数据的访问和操作必须经过云租户的授权 ， 授权必管理层面强制落实制度， 技术层面采用云堡垒进行审计。

a) 云服务商相关人员应签署商业行为准则协议 ， 确保对云租户数据的安全，确保云租户数据的隐私。（ 新增)选择云供应商时进行评估审查管理层面强制落实制度， 技术层面采用云堡垒进行审计。

b) 云平台定级应不低于云平台所承载的云租户业务系统的安全级别。

（ 新增)（ 云平台如何定级 ， 建议考虑清楚是否可以定级在写该条 ）

c) 选择云供应商时进行评估审查， 选择不低于业务系统定级的云平台

1 8、 系统建设及管理 / 服务商选择

a) 云服务商应满足服务水平协议(SLA) 要求;

b) 云服务商应在服务水平协议(SLA) 中规定云计算所能提供的安全服务的内容 ，并提供安全声明 ；

c) 云服务商应与云租户协同规定云服务商和云租户的权限与责任 ， 权限与责任细化到岗位 ；

d) 云服务商应与云租户协同规定违背服务水平协议 (SLA) 的惩罚措施 ,惩罚措施细化到岗位 ；

e) 云服务商需提供第三方合作商安签订公有云服务合同时明确相关条款等保内容 应对措施

全能力服务水平证明 ， 并提供对第三方安全能力服务水平监管证明。

f) 云服务商与云租户应签订隐私保护相关协议。

1 9、 系统建设及管理 / 服务商选择

a) 应要求信息系统、 组件或服务开发商提供描述相关功能的文档和信息;

b) 应要求信息系统、 组件或服务开发商为信息系统实施威胁和脆弱性分析;

c) 应要求信息系统、 组件或服务开发商提供所使用的安全措施的描述文档;

d) 应要求信息系统、 组件或服务开发商制定对安全措施有效性的持续监控的相关策略 ;

e) 应要求信息系统、组件或服务开发商提供事故应急预案 , 并将事故应急预案纳入云服务商的事件响应计划中 ;

制定相关安全管理制度并落实到系统建设、 运维过程中等保内容 应对措施

f) 云服务商应在开发商、 供应商或厂商不再对系统组件提供支持时采取相关措施。

20、 系统运维管理 / 监控管理和安全管理中心 a) 应对云平台的运行状况、 网络流量、 用户行为等进行监测和报警 , 形成记录并妥善保存 ;

b) 应建立对物理资源和虚拟资源进行统一调度和分配的规范或策略 ;

c) 云服务商应建立安全应急响应中心, 收集和处理云平台的安全漏洞 ;

部署 Web 、 系统、 数据库漏扫工具, 及时更新相关软件补丁

d) 应具备自动发现系统内虚拟主机和虚拟网络等各类虚拟资源的能力 ,通过图示的方法展现 , 并可对发现的虚拟网络拓扑进行实时监控和更新。

21 、 系统运维管理 / 网络和系统安全管理 a) 应建立虚拟资源申 请审查制度 ,保障重要虚拟机的资源使用 , 避免非法调用资源 ;

云安全运维管理制度; 运维管理流程;

操作流程; 操作日志审查

b) 应建立虚拟资源隔离策略文档 ,定期对策略进行一致性检查 ;

c) 应规定重要业务系统需要使用加固的操作系统镜像 ;

d) 应保证私有云的运维管理由投资建设方自行完成 , 或者由与产品提供商无任何商业关系的第三方完成。

e) 应保证公有云租户业务运维管理由租户自行完成 , 或者由与云服务商无任何商业关系的第三方完成。

云平台应可以定义多种角色, 并对不同的角色赋予不同的权限。

22、 系统运维管理 / 风险评估和漏洞修复

a) 云平台系统应具有独立的测试云。

云平台建设时规划独立的测试区域

23、 系统运维管理 / 密码管理

a) 应指定密钥的合法使用范围 ; 密钥管理规范和管理制度 b) 应合理选择密钥的存储方式 , 禁止云租户的密钥存放在云端 ;

密钥管理规范和管理制度

c) 应建立合理的密钥撤销机制 , 被撤销的密钥必须归档 ;

密钥管理规范和管理制度

d）对于公有云 ，应部署两套 CA。 面向公共的部分使用外部 CA。 内部的管理

安全域（ 管理网 ）部分使用组织自己的私有 CA。 两套 CA 不能混用。

e）应根据不同云的需求量 ，定制配置足够的熵源 ，防止实例的熵饥饿（ 根据云平台内所容纳的计算资源规模，选择合适的熵源 ，以确保有足够的硬件随机数来生成密钥 ）容量规划

24、 系统运维管理 / 备份和恢复管理

a）应制定对重要数据的存储限定在安全可控的地理范围内的相关要求。

物理位置规划， 数据中心选址分析

25、 系统运维管理 / 服务终止

a）租户与云服务商服务合约到期时 ,应完整地返还租户信息。

签订公有云服务合同时明确相关条款

b）在租户定义的时间内 ，清除云服务

平台上存储的租户信息 ，并确保不能采用技术手段恢复。

13.6.4 云安全体系架构设计

13.6.4.1 云整体安全逻辑架构

智慧园区大数据云中心专有云和互联网门户平台对于安全的需求， 可以从物理层、 虚拟化控制层以及安全服务层的角度进行安全体系的建设， 达到等级保护 3 级的设计要求。

13.6.4.2 云整体安全设计架构图

在考虑政务专有云安全防护需求时，更多的需要结合政务专有云内部的安全体系架构来进行落实。 政务专有云内部建立云内的网络安全防护机制， 在未经过授权允许的情况下， 政务专有云内各系统间默认情况下不能相互访问， 将不同应用系统加入到不同的安全区域， 不同安全区域之间的云主机网络默认隔离。 当需要互通时， 通过修改域间规则， 来打开互访通道。

针对与各个功能区域都部署了相应的安全产品，区域分别为：核心交换区、互联网出口区、政务网出口区、 云管理区、 数据库系统区、 业务系统区、 FC 存储区、 IP 存储区、 东西向安全资源池区。

13.6.4.3 云计算物理层安全

云计算物理层面临着对计算机网络与计算机系统的物理装备的威胁，是指由于周边系统环境和

物理特性导致的网络安全设备和线路的不可用， 从而造成所承载的网络应用不可用。 主要表现在自然灾害、 电磁辐射、 三防（ 防火、 防水、 防尘）及恶劣的工作环境方面， 而相应的防范措施包括抗干扰系统、 物理隔离、 防辐射系统、 供电系统的冗余设计和可靠性备份， 采取前后上下等多种通风方式。

13.6.4.4 虚拟化资源层安全

虚拟化软件导致的安全漏洞风险有两方面：

一方面， 以虚拟化应用程序本身可能存在的安全漏洞将影响到整个物理主机的安全。 黑客在利用漏洞入侵到主机系统之后， 可以对整个主机上的虚拟机进行任意的配置破坏， 从而导致系统业务不可用， 或者是将相关数据进行窃取 ， 如果黑客侵入了虚拟机配置管理程序， 则会直接影响到其管理的全部虚拟机的安全。

另一方面， 基于虚拟化环境开发的各种第三方应用程序的漏洞安全。 这些应用程序是云服务交付的核心组成， 包括 Web 前端的应用程序、 各种中间件应用程序及数据库程序等， 即使在传统网络安全环境下， 他们仍然会因为编程技术的缺陷而存在多个安全漏洞， 在云计算环境下， 这些安全漏洞会 续存在， 典型如各种 WEB 会话控制漏洞、 会话劫持漏洞及各种注入攻击漏洞。 同时为了适应或使用虚拟化环境下的各种 API 管理接口， 也可能产生一些新的安全漏洞。

云计算虚拟机流量交换的安全新风险： 在虚拟化环境下， 单台物理服务器上可以虚拟化出多个完全对立的虚拟机并运行不同的操作系统和应用程序， 各虚拟机之间可能存在直接的二层流量交换， 而这种二层交换并不需要经过外置的二层交换机， 管理员对于该部分流量既不可控也不可见，在这种情况下， 管理员需要判断 VM 虚拟机之间的访问是否符合预定的安全策略， 或者需要考虑如何设置策略以便实现对 VM 之间流量的访问控制。

针对虚拟化的资源安全防护手段主要从两个方面入手， 一方面通过漏洞扫描设备周期性的扫描主机及操作系统存在的漏洞， 从而进行相应的安全调整加固；

另一方面， 通过在网络中部署东西向安全资源池， 通过服务 技术把流量引出来引导安全资源池中进行安全防护。

13.6.4.5 多租户 IaaS 服务层安全

多租户环境下的基础安全服务主要体现在 IaaS 服务层。 IaaS 作为云计算的重要组成部分，其将基础设施包括网络、 存储、 计算等资源进行虚拟化等处理，能够为每个用户提供相对独立的服务器计算资源、 存储资源以及在承载网上设定专有的数据转发通道。

在智慧园区大数据云安全平台的建设过程中， 基于 IaaS 模型下的各种安全服务体系的建设其是重点所在， 根据现阶段的需求来看， 这部分服务主要包括针对云计算防火墙服务、 云计算负载均衡业务。 不同的租户可以根据自身的业务需求， 合理的选择部署云安全防火墙服务或者是防火

墙叠加负载均衡业务。 部署该安全服务后， 每个租户可以获得逻辑上完全属于自己的防火墙和负载均衡。 租户可以根据自身需求， 设定自身的各种安全防护策略， 生成自身独有的安全日志分析报告。 同时对于部分需要负载均衡的业务， 也可以设置独立的负载均衡的算法，以保证业务的可靠性运行。 当然， 考虑到应用层的安全风险一直是互联网的重点防护对象之一， 各种基于 web 应用层的安全攻击会导致用户业务系统的权限被窃取以及关键数据的泄露， 也可以考虑增加一些新的诸如 WAF 、 IPS 入侵检测等增值服务， 用户可以根据自身业务系统的安全级别合理选择是否租用该漏洞防护服务等。 这部分的内容后续将作为重点进行论述。

13.6.4.6 PaaS/SaaS 应用层数据安全

在云安全体系的建设过程中， PaaS 和 SaaS 的安全建设也非常重要。 和 IaaS 的建设思路不同， PaaS 的安全建设， 其关键在于平台开放的思想下， 开发者应用平台及数据库系统对于多开发者数据安全的适配。 典型问题包括针对开发者的用户身份认证， 开发者的平台和数据库的访问使用权限控制， 不同开发者数据的安全隔离、 及操作行为审计等内容。 为此需要在数据库的开发及平台应用环境开发过程中考虑到上述安全风险的防护。 而在 SaaS 模型下， 应用系统级的多租户共享涉及到的应用层安全问题，除了多租户身份认证和权限控制及数据库安全隔离等需求外，还需要考虑针对应用环境的代码级的安全审计等问题，确保提供给租户的应用程序本身的安全具备很高的水平， 不会轻易被黑客等攻击者利用其内在的各种安全漏洞。 在本次的智慧园区大数据云建设过程中， 这部分的安全通过合理配置数据库及应用程序来进行保证。

13.6.5 各功能区域架构设计

13.6.5.1 核心交换区

（1） 组网模式

核心交换区在不改变原有网络基础架构的前提下，在核心交换区域的核心交换机旁挂相应的安全设备， 如 WA、F 时加固了整体云平台的安全性。

（2） 功能概述

核心区的功能概述如下：

LB 等， 来保证核心交换区的安全合规性， 同 WAF ： 专注于 7 层防护， 采用最为先进的双引擎技术， 采用用户行为异常检测引擎、 透明代理检测引擎相结合的安全防护机制实现各类 SQL 注入、 跨站、 挂马、 扫描器扫描、 敏感信息泄露、 盗 行为等攻击防护， 并有效防护 0day 攻击，支持网页防篡改。 可以帮助用户解决目前所面临的各类网站安全问题 LB: 负载均衡可以实现对网络设备和服务器带宽的有效扩展， 充分利用多台服务器的业务处理能力， 通过合理的调度算法和健康检查算法， 可以有效感知服务器的负载并将业务流量调度到最恰当的服务器上， 从而提

高网络的灵活性和可用性。

13.6.5.2 互联网出口区

（1 ）组网模式

互联网出口区部署防火墙、 IPS、 路负载均衡、 上网行为审计和防 DDoS，在智慧园区大数据云中心的内网和外网之间构建一套坚固的安全屏障。

（2） 功能概述

互联网出口区的功能概述如下：

配置 M9000 防火墙， 支持外部攻击防范、 内网安全、 流量监控、 邮件过滤、网页过滤、 应用层过滤等功能， 能够有效的保证网络的安全；

负载均衡： 提供出口 路负载均衡， 通过 M9000 防火墙的 路负载均衡功能模块实现。

配置入侵防御系统功能模块能提供强大的攻击防护和流量模型自学习能力，当攻击发生、 或者短时间内大规模爆发的病毒导致网络流量激增时， 能自动发现并阻断攻击和异常流量， 以保护路由器、 交换机、 VoIP 系统、 DNS 服务器等网络基础设施免遭各种恶意攻击， 保证关键业务的通畅， 检测和阻断来自外部的攻击。

配置防 DDoS： 通过专业的防 DDoS 设备来帮助部署在云上的主机等资源抵御 DDoS 攻击， 攻击类型包含网络层、 传输层、 应用层的所有分布式拒绝服务攻击，并实时通知用户攻击行为。

配置上网行为审计设备， 支持应用层内容过滤及审计， 可以有效的识别网络中各种 P2P 模式的应用， 并且对这些应用采取限流的控制措施， 有效保护网络带宽； 支持邮件过滤， 提供 SMTP 邮件地址、 标题、 附件和内容过滤； 支持网页过滤， 提供 HTTP URL 和内容过滤。

13.6.5.3 云管理区

（1） 组网模式

在云管理平台子区以及带外管理区配置相应的安全设备， 如安全管理检测中心以及堡垒机等来保证云整体架构在管理整个云基础架构系统的时候， 加固了整体云平台的安全性。

（2） 功能概述

云管理区的功能概述如下：

堡垒机： 可以通过堡垒机对运维接口统一， 进行统一的账户管理、 统一认证、进行运维的会话命令等进行审计、 对权限进行精细化控制等， 从而实现身份管理、访问控制、 权限控制、 操作审计。

云安全监测中心： 可以安全管理中心基于先进的深度挖掘及分析技术， 集安全事件收集、 分析、 响应等功能为一体， 解决了网络与安全设备相互孤立、 网络安全状况不直观、 安全事件响

应慢、 网络故障定位困难等问题， 使 IT 及安全管理员脱离繁琐的管理工作， 极大提高工作效率，能够集中精力关注核心业务。

漏洞扫描： 漏洞扫描设备可以对网络内的数据库、 WEB 、 操作系统进行探测并扫描， 对可能存在漏洞， 如弱口令、 注入漏洞等， 进行综合分析， 并支持授权深度扫描。 系统漏洞扫描：针对主机操作系统、 中间件、 主流网络设备、 浏览器等进行脆弱性扫描， 分析潜在风险并提供加固建议。

13.6.5.4 数据库系统区

(1) 组网模式

在数据库区域的汇聚交换机层面旁挂相应的安全设备， 如数据库审计来保证数据库区域的安全合规性， 同时加固了整体云平台的安全性。

(2) 功能概述

数据库系统区的功能概述如下：

① 数据库审计： 实现细粒度审计、 精准化行为回溯、 全方位风险控制， 为核心数据库提供全方位、 细粒度的保护功能， 可帮助用户带来如下价值点：

全面记录数据库访问行为， 识别越权操作等违规行为， 并完成追踪溯源跟踪敏感数据访问行为轨迹， 建立访问行为模型， 及时发现敏感数据泄漏

检测数据库配置弱点、 发现 SQL 注入等漏洞、 提供解决建议为数据库安全管理与性能优化提供决策依据提供符合法律法规的报告， 满足等级保护、 内控等审计要求

13.6.5.5 东西向资源池区

(1) 组网模式

在网络中单独部署一个东西向安全资源池区， 部署 NFV 产品形态的 VFW、 VLB。

(2) 功能概述

业务系统区的功能概述如下：

虚机间的流量访问控制及威胁检测依赖 NFV 资源池。

NFV 资源池中的 VFW 支持透明模式部署， 满足内部 VM 间安全防护需求； 支持透明模式部署，提供对数据中心内 VM 间流量防护：

1） 设置安全策略控制对 VM 虚拟机之间的访问， 对这些 VM 之间的流量访问进行允许或禁止；

2） 对 VM 之间的流量互访进行攻击检测， 及时发现内部攻击行为。

虚机间的流量要想按需调度到 NFV 资源池中， 要依赖于 SDN+VxLAN 技术， 还要依赖服务 技术。 数据报文在网络中传递时， 需要经过各种各样的业务节点，才能保证网络能够按照设计要求，提供给用户安全、 快速、 稳定的网络服务。 网络流量按照业务逻辑所要求的既定的顺序， 经过

这些业务点， 这就是服务 。

传统网络中的防火墙、 负载均衡器等业务节点和网络拓扑有 密的耦合， 部署较为复杂， 在服务 变更、 扩容时， 都需要改动网络拓扑， 并重新进行网络设备的配置。 随着 NFV 技术的的发展， 业务节点可以方便的部署在虚拟化网络甚至直接安装到服务器中。 为了引导网络中的业务报文次序通过虚拟化网络中的多个业务节点处理后再进行转发， 需要 SDN 的服务 功能来实现。 服务 是支撑虚拟化、 业务网络可编程的关键技术。

简单来说， 本项目中采用的 VFW 实际是作为一个特殊的虚拟机运行在虚拟平台中， 正常情况下 VM 间访问流量直接经过 vSwitch 互访， 当需要对其进行安全防护时， 管理员配置通过 SDN 控制器创建服务 策略， 当 VM 间第一次发生交互流量时， vSwitch 会向控制器申请的引流策略（包含服务 策略的流表） ， 策略下发后， vSwitch 根据流表内容对流量进行匹配， 将需要防护的流量引流到 VFW 中，由 VFW 对虚拟机间流量进行防护处理，最后经 VFW 处理过的流量再回到 vSwtich 中进行正常转发；

13.6.5.6 虚拟主机安全防护

针对虚拟主机的安全防护采用虚拟化安全管理系统，虚拟化安全管理系统是面向多种虚拟化平台推出的虚拟化统一威胁管理系统， 针对虚拟化中出现的杀毒风暴、 更新风暴及虚拟机差时防护等问题以无代理的方式提供全时的安全防护，并可以对宿主机系统提供全面的安全保障， 从而形成跨平台的虚拟化安全综合解决方案。

13.7 云安全建设方案

13.7.1 物理安全

13.7.1.1 供配电系统

机房的供配电系统要保证对机房内的主机、 服务器、 网络设备、 通讯设备等的电源供应在任何情况下都不会间断， 做到无单点失效和平稳可靠， 要提供两路以上的市电供应， N+1 冗余的自备发电机系统， 要求保证足够时间供电的 UPS 系统。

13.7.1.2 防雷接地

为了保证机房的各种设备安全， 要求机房设有四种接地形式， 即计算机专用直流逻辑地、 配电系统交流工作地、 安全保护地、 防雷保护地。

13.7.1.3 消防报警及自动灭火

为实现火灾自动灭火功能， 在机房的各个地方， 要求设计火灾自动监测及报警系统， 以便能自动监测火灾的发生， 并且启动自动灭火系统和报警系统。

13.7.1.4 门禁

机房要求建立实用、 高效的门禁系统， 门禁系统需要注意的原则是安全可靠、 简单易用、 分级制度、 中央控制和多种识别方式的结合。

13.7.1.5 保安监控

机房的保安监控包括几个系统的监控： 闭路监视系统、 通道报警系统和人工监控系统。

13.7.2 网络安全

13.7.2.1 网络边界安全

智慧园区大数据云计算环境下的边界安全主要分为： 不同业务区域之间安全边界、 不同租户之间的安全边界、 云平台南北向网络流量安全边界、 云平台东西向网络流量的安全边界。

同业务区域之间安全边界规划设计：

依据业务应用系统服务和使用的对象不同， 将其划分为 xxx 网安全域和互联网接入安全域，此两个业务区域之间安全设计如下：

xxx 网安全域和互联网接入安全域之间通过网闸或光闸实现物理隔离。

不同租户之间的安全边界规划设计：

不同租户在云管理平台上账号安全通过账号名称、 账号密码和账号权限实现安全隔离。

不同租户在云平台上的资源通过虚拟私有云（ VPC） 技术实现逻辑隔离。

云平台南北向网络流量安全边界规划设计：

云平台中， 各个租户业务应用系统南北向业务流量安全通过硬件虚拟化防火墙实现逻辑隔离。

云平台东西向网络流量的安全边界规划设计：

云平台中， 各个租户业务应用系统东西向业务流量安全通过“ SDN 技术” +“服务 技术”

+“NFV 架构虚拟化防火墙” 实现逻辑隔离。

13.7.2.2 防火墙

13.7.2.2.1 功能设计

1、 通过在 xxx 网和互联网安全域边界部署专业的防火墙设备， 来支持攻击防范、 访问控制、安全域划分、 黑名单等功能， 有效的保证网络的安全， 实现访问的精准控制。

2、 通过在安全区域间使用标准或扩展访问控制规则， 借助报文中 UDP 或 TCP 端口等信息实现对数据包的过滤， 支持按照时间段进行过滤。

3、 通过检查应用层协议信息 （如 RAWIP/ICMP/ICMPV6U/ DP-LITE/ SCTP 及其它基于 TCP/UDP 协议的应用层协议） ， 并监控基于连接的应用层协议状态， 动态的决定数据包是被允许通过或者是被丢弃。

4、 提供虚拟防火墙功能， 可为虚拟防火墙划分独立的 CPU、 内存、存储资源； 虚拟防火墙能够支持和云平台联动， 在云平台上按需申请和分配安全资源， 做到安全策略的统一编排提高资源利用率和安全编排能力。

5、 提供支持安全集群功能， 可以将多台物理设备虚拟化为 1 台逻辑设备； 设备集群后能完全作为 1 台设备来统一配置管理。

6、 所提供设备为专业的安全设备， 非交换机 +安全插卡方式； 整机槽位数≥ 1 0； 其中独立的主控引擎槽位数≥ 2， 独立交换引擎槽位数≥ 3， 独立业务槽位数≥ 4； 吞吐量≥ 40G， 并发连接数≥ 3000 万，每秒新建连接≥ 60 万， 配置虚拟防火墙许可≥ 256 个； 具备公安部《计算机信息系统安全专用产品销售许可证》 ； 配置冗余主控引擎、 冗余交换引擎、 冗余电源， 至少提供 8 个万兆光口及配套光模块。

13.7.2.2.2 部署设计

1 、 部署条件

互联网区和 xxx 网区防火墙以硬件方式部署， 分别部署在网络边界和旁挂在核心交换机旁做策略路由的引流， 进行安全防护， 边界防火墙提供全局访问控制以及地址转换服务； 核心旁挂防火墙需要开启多租户实例功能， 为每租户提供基于虚拟化实例的租户防火墙和实例化 VPN 接入服务。

2、 策略设置

智慧园区大数据云边界防火墙面向外部提供基于端口的地址转换， 针对不同系统的需求， 开放有限的端口映射， 并配置全局安全访问控制策略， 对黑名单地址进行过滤； 核心旁挂防火墙需要开启多租户防火墙功能， 针对每租户的策略需要细化到端口级别； 需要配置单独的带外管理口，业务口推荐使用捆绑机制。

3、 部署数量及位置

互联网区核心交换机旁挂、 政务外网区核心交换机旁挂， 通过策略路由进行流量牵引。

4、 服务模式

智慧园区大数据云边界防火墙提供全局防护与地址转换服务核心旁挂防火墙在 VPC 中为每租户提供租户级别的防火墙和 VPN 服务

13.7.2.3 抗拒绝服务攻击（ DDOS 攻击） 设计

13.7.2.3.1 功能设计

1、 通过专业的防 DDoS 设备来帮助部署在云上的主机等资源抵御 DDoS 攻击， 可防护各类基于网络层、 传输层及应用层的拒绝服务攻击， 如 SYN Flood、 UDP Flood、 UDP DNS Query Flood、(M)Stream Flood 、ICMP Flood、 HTTP Get Flood 以及连接耗尽等常见的攻击行为。

2、 能够提供完备的异常流量检测、 攻击防御、 设备管理、 报表生成、增值运营等功能；

3、 能够支持包括串联、 串联集群、 旁路以及旁路集群等不同部署方式。 旁路部署下支持多种路由协议进行流量的牵引和回注， 满足各种复杂的网络环境下的部署需求。

4、 所提供设备设备吞吐量≥ 6G。

13.7.2.3.2 部署设计

1 、 部署条件

在互联网出口区域通过 BGP 牵引方式进行流量清洗， 需要同时部署检测系统和清洗系统， 检测设备对用户业务流量进行分析监控。当用户遭受到 DDoS 攻击时，检测设备上报给清洗设备，将清洗设备发送牵引路由给边界路由器， 对牵引过来的用户流量进行清洗， 并将清洗后的用户合法流量回注到云内。

2、 策略设置

DDOS 产品需开启的策略包括：网络业务流量监控和分析、 安全基线制定、 安全事件通告、 异常流量过滤、 安全事件处理报告等。 通过串行或旁路引流部署， 减轻来自于 DDoS 攻击流量对智慧园区大数据云出口造成的压力， 提升带宽利用的有效性。

3、 部署数量及位置

互联网出口部署的 DDOS 产品需要通过与边界的路由交换设备启用 BGP 协议， 并通过 netflow 方式将流信息发送到 DDOS 的检测组件中进行流模型匹配。

4、 服务提供方式

DDOS 产品主要以硬件形态的方式进行部署， 以全局防护的方式进行交互， 主要是对互联网区域内的服务器和通讯 路进行保护。

13.7.2.4 VPN 安全接入设计

13.7.2.4.1 功能设计

1、 能够使用 IPSec VPN 和 SSL VPN 等 VPN 接入方式接入 xxx 网， 以实现多分支接入和移动办公。

2、 对于 SSL VPN 用户认证可使用本地认证、 radius 认证、 LDAP 认证、 USBkey 认证、 证书认证等认证方式。

3、 终端可使用终端可使用 WindowsXP\Windows7\Windows8 等操作系统来登录 SSL VPN 系统。

4、 终端可使用 IE、 Firefox 、 Safari 、 Google Chrome 浏览器来登录 SSL VPN 系统。

5、 所提供设备应至少提供 8 个千兆光口、 8 个千兆电口、 2 个万兆光口， 至少具有 2 个扩展槽位。 吞吐量≥ 8G， 配置 1 000 个 SSL VPN 接入用户授权， IPSec 隧道数至少为 6K。

13.7.2.4.2 部署设计

1 、 部署条件

VPN 产品部署在 xxx 网边界，重要系统的访问路径推荐部署 2 套作为主备，通过 xxx 网 VPN 连入时， 采用 IPSec 或 SSLVPN 方式互联，加密方式推荐采用符合国家相关加密认证标准的加密算法， 虚拟路由需要做精细化隔离， 通过变长子网掩码对路由的目标地址做精细化限制，另外 VPN 需要配置单独的带外管理口， 业务口推荐使用捆绑机制。

2、 策略设置

隧道封装模式主要通过路由策略控制对子网的访问， 通过变长子网掩码对路由目的范围做最小化控制。

应用发布方式主要将 B/S 业务进行 HTTPS 的封装， 需要限定对外发布的端口和服务的路径，并通过与外部认证系统完成终端接入用户的认证。

3、 部署数量及位置

在 xxx 网区域旁挂于汇聚交换机， 单臂部署， 推荐两台做冗余。

4、 服务提供方式以硬件方式部署， 开启多租户虚拟化功能， 为每个租户分配 VPN 实例。

13.7.2.5 网络漏洞扫描设计

13.7.2.5.1 功能设计

1 、 智能端口识别

能对开放端口运行的服务进行智能服务识别 ， 而不是固定地依据默认值去判断

2、 信息抛出

支持保存扫描脚本中动态抛出的信息， 能够获取主机的 netbios 名、 主机名、 工作组 / 域名、 MAC 地址、 SID 名、 用户名列表、 弱密码、密码不过期、 密码未改变、 共享列表、 系统服务列表、 注册表完全访问等信息

3、 断点恢复

在扫描程序运行到一半的时候如果系统意外掉电等， 可以通过查看扫描状态进行重新扫描或者续扫描

4、 漏洞库

漏洞库按服务分不低于 40 种类别， 按风险分为 急、 高、 中、低、 信息五个级别， 基于国际 CVE 标准建立， 漏洞数量不小于 30000 条

5、 密码分析

对较弱的密码口令进行扫描并产生报告。 同时可以利用扫描到的弱口令对系统进行授权深度扫描

13.7.2.5.2 部署设计

1 、 部署条件

由于漏洞扫描产品是采用模拟渗透的方式进行漏洞检查和弱口令检查， 漏扫的任务应建立在最小的扫描范围， 不建议扫描的流量经过核心交换机到达整网， 通过部署在管理网络连接管理交换机进行带外的安全扫描。

2、 策略设置

建议开启所有的策略分别对各网段进行扫描， 扫描完成后生成报表并且存储在本地。

3、 部署数量及位置

建议部署管理区， 通过管理区域交换机与被扫描资产的带外管理口连接。

4、 服务提供方式

漏扫产品以软件方式部署， 可以为每租户独立安装， 也可安装在智慧园区大数据云的管理网络， 对基础设施进行漏洞扫描。

13.7.2.6 负载均衡设计

13.7.2.6.1 功能设计

1、 提供 路负载均衡、 服务器负载均衡功能。

2、 支持包括轮询、 加权轮询、 最小连接、 加权最小连接、 随机、 加权随机、 源地址 Hash、源地址端口 Hash、 目的地址 Hash、 UDP 报文净荷 Hash、 优先级等负载均衡调度算法。

3、 提供 TCP 连接复用功能； 提供 HTTP 压缩功能。 提供 SSL 卸载功能， SSL 卸载性能≥ 10000TPS。

4、 支持将一台设备虚拟化为多台设备使用。

13.7.2.6.2 部署设计

路负载均衡功能通过 M9006 多业务安全网关上的 路负载均衡功能模块实现， xxx 网和互联网区各部署 2 套。

服务器负载均衡以硬件方式交付， 通过 xxxSecPath L5000-C 设备实现， 旁挂在互联网区核心交换机上。

13.7.2.7 入侵防护系统设计

13.7.2.7.1 功能设计

1、 通过对访问互联网的网络数据流进行 2 到 7 层的深度分析， 能精确、 实时地识别并阻断或限制黑客、 蠕虫、 病毒、 木马、 DoS/DDoS、扫描、 间谍软件、 协议异常、 网络钓鱼等网络攻击或网络滥用， 以起到入侵防范的目的。

2、 提供 3 年特征库升级服务， 攻击特征库数量要≥ 3000+、 病毒特征库数量要≥ 8000+、支持的协议识别数量≥ 800+， 要包含主流操作系统、 主流网络设备、 主流数据库系统、 主流应用软件系统的全部漏洞特征， 同时也要包含蠕虫、 病毒、 木马、 DoS/DDoS 、 扫描、 间谍软件、网络钓鱼等网络攻击或网络滥用特征。

3、 可结合模式特征匹配、 协议异常检测、 流量异常检测、 事件关联等多种技术， 能识别运行在非标准端口上的协议， 准确检测入侵行为。

检测到攻击报文或攻击流量后， 支持阻断、 限流、 捕获原始报文等常规响应方式； 支持隔离、 Web 重定向等响应方式， 以实现第一时间隔离有安全威胁的主机。

13.7.2.7.2 部署设计

通过 M9006 多业务安全网关上的 IPS 功能模块实现， 在 xxx 网和互联网区各部署两套。

13.7.2.8 网络安全审计设计

13.7.2.8.1 功能设计

堡垒机

可以通过堡垒机对运维接口统一， 进行统一的账户管理、 统一认证、 进行运维的会话命令等进行审计、 对权限进行精细化控制等， 从而实现身份管理、 访问控制、 权限控制、 操作审计。

上网行为审计系统

1、 支持自定义关键字对象， 在行为审计的时候可选择“包含” 、“不包含”、“等于” 、“不等于” 四种匹配模式， 匹配类型包含关键字和数字。

2、 支持收集网站访问日志， 记录用户所有访问网站行为； 支持收集搜索引擎日志， 记录用户的搜索内容； 支持收集 IM 通讯软件日志，记录用户登陆、 注销、 收发消息、 收发文件等行为； 支持收集邮件日志， 记录邮件发件人、 收件人、 主题、 正文、 附件等信息。

支持网络社区应用管控的精细化管理，可管控“登录” 、“注销” 、“发表”、“搜索” 、“举报” 、 “上传” 、 “私信” 、 “删除”等行为。

3、 支持路由模式、 透明（网桥） 模式、 混合模式， 部署模式切换无需重启设备。

4、 支持应用、 用户流量统计， 应用流量支持趋势图、 饼状图呈现，可查看某一应用的流量趋势图和其 Top 流量用户。

5、 所提供设备采用多核架构设计， 内置 Bypass 模块， 在设备断电重启时， 可自动切换到 Bypass 状态， 当设备恢复时， 可自动切换回工作状态；

日志审计系统

1 、 能对操作系统、 数据库、 中间件、 应用进行监控， 并通过列表展示应用详情， 包括应用名称、 应用类型等风险状况。

2、 支持业务定义， 包含指定业务名称、 描述、 优先级、 联系人、 业务中包含的应用和服务器、 业务中包含的网络设备等信息， 并以列表形式显示各业务的风险状况。

3、 能对最近一小时的事件进行汇总分析和展现。 支持按设备名称、 TOP 个数、 业务等作为分析条件。 提供攻击源 TOP、 目的 TOP、 产生事件最多的设备 TOP、 产生最多的事件 TOP、 事件趋势、 攻击协议 TOP 等分析图表。

4、 能管理平台支持展示网络拓扑和安全拓扑， 支持完整攻击拓扑溯源， 可展示攻击路径上的交换、 路由、 安全设备。

13.7.2.8.2 部署设计

堡垒机

1 、 部署条件

运维审计系统 （ 堡垒机） 在云服务方基础设施层部署相对简单，该系统需要一个业务口和一个管理口。 管理口只要路由可达即可访问， 业务口只需和被管理目标路由可达。 一般建议部署在独立的管理网络中， 与管理网交换机相连， 并可以访问被管理资产的带外管理口，同时为了保证堡垒机作为运维操作的唯一出口， 需要通过设置网络管

理区的防火墙策略对运维协议进行地址限制。

虚拟堡垒机需要集群部署在独立的服务器当中， 并为每个 VPC 多分配一个管理 Vxlan ， 这个 Vxlan 就是租户管理员的访问路径， 同时在南北向防火墙上面阻断租户管理员远程访问 VPC 内其他非堡垒机资源的流量， 通过 SDN 控制器进行访问配置， 允许一个租户的虚拟堡垒机可以访一个 VPC 内部的多个不同 Vxlan 内的资源。

2、 策略设置

配置主从账号， 将在堡垒机分配运维人员的主账号用于单点登录和管理员认证， 同时录入从账号用于堡垒机通过运维协议远程连接目标主机。

3、 部署数量及位置

在管理区单臂部署 1 套， 专为云服务商进行底层资源管理使用；

云租户可以使用虚拟化版本， 但是建议每个 VPC 单独使用一套， 租户由云平台申请堡垒机资源，

4、 服务提供方式

以硬件方式提供：部署在智慧园区大数据云的管理网络中，与管理交换机相连，提供 IaaS 层的安全运维以 NFV 方式提供： 可以为 VPC 内的租户安装部署虚拟化版本。

上网行为审计系统

以硬件方式提供， 在两个生产中心的互联网区各部署一套。

日志审计系统

以硬件方式提供， 通过 xxxSecCenter A***0 安管平台实现， 部署在管理区。

13.7.2.9 跨网安全设计

13.7.2.10 功能设计

1、 用于 xxx 网和互联网之间数据摆渡使用， 有效地隔断 xxx 网和互联网之间的直接连接，

防止信息无限制交换。

2、 采用三机系统结构， 内外端机为 TCP/IP 网络协议的终点， 阻断 TCP/IP 协议的直接贯通。 内外端机之间采用专用硬件和专用协议进行连接， 不可编程。

3、 只能通过内端机上的管理口对设备进行配置， 外端机上禁止配置管理。

4、 提供安全上网、 安全邮件、 文件传输、 文件同步、 数据库访问、数据库同步功能。

5、 支持异构数据结构以及代码语义的转换规则定义， 并实现源数据到目标数据之间的实时数据交换， 支持数据整合业务。

13.7.2.11 部署设计

在 xxx 网和互联网之间部署硬件网闸或光闸实现。

13.7.3 主机安全

13.7.3.1 主机访问控制设计

13.7.3.1.1 功能设计

1 、 主机防火墙

在操作系统内核层实现文件、 注册表、 进程、 服务、 网络等对象的强制访问控制， 可配置针对以上对象不同的访问策略来保护系统和应用资源， 即使是系统管理员也不能破坏被保护的资源。

2、 防格式化保护机制

保护功能开启时， 可防止病毒和入侵者恶意格式化磁盘， 同时降低管理员意外格式化磁盘的风险。

3、 完整性检测

对文件和服务进行完整性检测， 并可设置定期检测项目， 当发现文件或者服务篡改时进行报警并发现哪些文件发生改变。

4、 系统资源监控与报警

对系统的 CPU、 内存、 磁盘、 网络资源进行监控， 当这些资源的使用状况超过设置的阀值时将进行报警， 以提前发现资源不足、 滥用等问题。

13.7.3.1.2 部署设计

1 、 部署设计

通过对物理主机系统、 虚拟化主机系统、 虚拟化操作系统进行安全加固

2、 安全策略

对远程接入用户进行补丁、 杀毒软件、 进程、 应用等控制对智慧园区大数据云内部服务器，推荐少量功能开启， 包括注册表监控和启动项监控

3、 服务提供方式

服务方式为 VPC 级别的服务申请

13.7.3.2 主机防病毒设计

13.7.3.2.1 功能设计

1 、 所提供产品支持无代理底层网络数据包过滤， 不需要在虚拟服务器或虚拟桌面中部署安全防护代理。

2、 能够为云主机提供病毒与木马防护服务， 能够提供官方病毒码下载地址。

3、 所提供产品厂商必须为国内厂商， 有独立的病毒响应中心、 研发中心。

4、 能够为云主机提供恶意代码防范服务。

5、 最新病毒爆发时， 产品厂商必须提供应急技术支持， 如电话、 手机短信、 邮件等方式。

13.7.3.2.2 部署设计

主机防病毒客户端直接布署在物理机或虚拟化上， 服务交付方式为 VPC 内系统保护， 无全局防护需求。

13.7.3.3 主机安全审计系统设计

13.7.3.3.1 功能设计

1、 通过软件形式提供云主机的安全审计服务， 能够支持和云平台联动， 云租户客户通过云平台申请云主机安全审计服务。

2、能记录用户在目标设备上进行的 Telnet 、SSH、RDP、VNC、Http 、Https 、FTP、SFTP、

SCP 等协议的所有操作行为， 还能审计第三方客户端工具的操作， 如 citrix 客户端、 PL/SQL、 SQLPLU、S TOAD 等工具。 可对图形、 字符、 应用、 文件四种类型进行审计。

3、 能对运维用户和运维资产进行权限授权， 支持一对一、 一对多、多对多授权。

4、 能够自动学习资产、 账户密码、 用户权限关系； 将学习到的资产可以自动添加到资产列表中， 并列出每个用户的权限范围， 方便管理人员快速审核和授权。

5、 能对运维操作事件进行监控， 对于正在进行的运维操作会话， 支持实时监控， 能够手工切断实时会话； 支持 Vi 、 aix 下 smit 、 rhel 下 setup 等图形或菜单操作进行全程同步监控；能够监控审计运维用户在什么时间、 什么 IP 登录了什么资产， 什么时间登出， 并记录完整的从登录到退出的整个过程。

6、 能对文件传输的过程进行记录： 支持记录 SFTP/FTP 传输的原始文件， 并可下载查看； 能通过系统控制是否需要记录原始文件，或者根据文件大小记录原始文件；可以对文件进行 sha1 值签名， 重复的文件可以不记录。

13.7.3.3.2 部署设计

在 xxx 网和互联网的管理区分别部署一台硬件堡垒机设备对主机实现安全审计。

13.7.4 虚拟化安全

13.7.4.1 虚拟机访问控制设计

13.7.41.1 虚拟机访问控制设计

1、 轻量级部署

支持 VMware ESX、i Linux KVM、 XXX CAS 等多个主流的虚拟平台， 充分发挥虚拟化的优势，实现快速部署、 批量部署、 镜像备份、 快速恢复， 并且能够灵活迁移。

提供 ISO 镜像、 OVA 模板、 IPE 等多种发布格式， 适应各种环境下的部署

2、 防火墙功能

支持包过滤。 借助报文中优先级、 TOS、 UDP 或 TCP 端口等信息作为过滤参考， 通过在接口输入或输出方向上使用标准或扩展访问控制规则， 可以实现对数据包的过滤。 同时， 还可以按照时间段进行过滤。

支持应用层状态包过滤（ ASPF） 功能。 通过检查应用层协议信息（如 FTP、 HTTP、 SMTP 、

RTSP 及其它基于 TCP/UDP 协议的应用层协议） ， 并监控基于连接的应用层协议状态， 动态的决定数据包是被允许通过防火墙或者是被丢弃。

支持丰富的攻击防范技术。 包括： Land、 Smurf、 Fraggle 、 Pingof Death、 Tear Drop、IP Spoofing 、 IP 分片报文、 ARP 欺骗、ARP 主动反向查询、 TCP 报文标志位不合法超大 ICMP 报文、 地址扫描、 端口扫描等攻击防范， 还包括针 SYNFlood 、UDPFlood 、ICMP Flood 等常见 DDoS 攻击的检测防御。

支持多种 VPN 业务， 如 L2TP VPN、 IPSec VPN、 GRE VPN 等，可以针对客户需求通过拨号、租用线及 VLAN 或隧道等方式接入远端用户， 构建 Internet 、 Intranet 、 Access 等多种形式的 VPN。 结合防火墙、 AAA、 NAT、 及多种 QoS 等技术， 防火墙可以确保在开放的 Internet 上实现安全的、 满足可靠质量要求的私有网络。

支持安全区域管理。 可基于接口、 VLAN 划分安全区域。

支持静态和动态黑名单。

支持丰富的路由协议。 支持静态路由、 策略路由， 以及 RIP、OSPF 等动态路由协议。

13.7.4.1.2 部署设计

1、 部署条件

虚机间的流量要想按需调度到 NFV 资源池中， 要依赖于 SDN+VxLAN 技术， 还要依赖服务 技术。 数据报文在网络中传递时，需要经过各种各样的业务节点， 才能保证网络能够按照设计要求

2、 策略配置

设置安全策略控制对 VM 虚拟机之间的访问， 对这些 VM 之间的流量访问进行允许或禁止；

对 VM 之间的流量互访进行攻击检测， 及时发现内部攻击行为 VFW 实际是作为一个特殊的虚拟机运行在虚拟平台中， 正常情况下 VM 间访问流量直接经过 vSwitch 互访， 当需要对其进行安全防护时， 管理员配置通过 SDN 控制器创建服务 策略， 当 VM 间第一次发生交互流量时， vSwitch 会向控制器申请的引流策略 （包含服务 策略的流表） ， 策略下发后， vSwitch 根据流表内容对流量进行匹配， 将需要防护的流量引流到 VFW 中， 由 VFW 对虚拟机间流量进行防护处理， 最后经 VFW 处理过的流量再回到 vSwtich 中进行正常转发

3、 部署数量及位置

推荐每个 VPC 一套安全资源池， 安全资源池中可包含 vFW 和 vLB， 其中 vFW 为必配产品， 推荐部署在单独的物理服务器当中，与租户的世界业务划归不同的 Vxlan ， 由 SDN 控制器进行流表引流。

4、 服务交付方式

建议每 VPC 使用独立的安全资源池进行虚拟机之间的访问控制。

13.7.5 应用安全

13.7.5.1 应用漏洞扫描设计

13.7.5.1.1 功能设计

安全漏洞检测： 支持 OWASP TOP 1 等 0 主流安全漏洞的自动检测网页木马检测： 对各种挂马方式的网页木马如 Iframe 、 CSS、 JS、SWF 、 ActiveX 等， 对网页木马传播的病毒类型做出准确剖析和网页木马宿主做出精确定位。

自动取证： 包括后台数据库中的数据提取、 执行控制台命令、 获取注册表数据、 获取目录树、 数据库操作、 备份数据库、 远程文件下载、 文件上传等。

手工取证： 支持对所有扫描结果中的存在的安全漏洞进行手工取证， 诸如跨站攻击测试、 表单绕过等无害攻击测试等

配置审计： 通过当前弱点获取数据库的相关敏感信息， 对后台数据库进行配置审计， 如弱口令、 弱配置等。

屏幕锁定功能： 在扫描过程中， 可以在不停止扫描的情况下锁定屏幕。 用户可自行设置系统超时时间

13.7.5.1.2 部署设计

1 、 部署条件

由于漏洞扫描产品是采用模拟渗透的方式进行漏洞检查和弱口令检查，漏扫的任务应建立在最小的扫描范围， 不建议扫描的流量经过核心交换机到达整网， 通过部署在管理网络连接管理交换机进行带外的安全扫描。

2、 策略设置

建议开启所有的策略分别对各网段进行扫描， 扫描完成后生成报表并且存储在本地。

3、 部署数量及位置

建议部署安全管理区域， 通过管理区域交换机与被扫描资产的带外管理口连接。

4、 服务提供方式

漏扫产品以软件方式部署， 可以为每租户独立安装， 也可安装在智慧园区大数据云的管理网络， 对 WEB 应用进行漏洞扫描。

13.7.5.2 WEB 应用防护设计

13.7.5.2.1 功能设计

检测算法： 可精确识别包括注入、 XSS 等 OWASP Top 1 0 WE 通 B 用攻击， 有效应对盗 、 跨站请求伪造等 WEB 特殊攻击 CC 防护： 支持 JS 的挑战模式， 识别人机互访； 自学习用户流量模型， 如新建、 并发等参数， 根据流量模型监控流量是否异常， 按需开启 CC 防护策略； 基于地理位置的识别， 可设置不同地理区域的防护单元。

13.7.5.2.2 部署设计

1 、 部署条件

可以通过透明串接、 反向代理、 路由模式等方式接入网络中，即可对应用层 HTTP 流量进行安全防护。

2、 策略设置

黑名单引擎策略设置： 通过预定义策略及自定义规则 （可根据用户对于安全的需求自行添加规则， 可基于不同条件组合， 如 HTTP 头部各字段、 URL 地址、 post 内容、 文件类型等字段，实现复杂的规则需求， 并设置阻断、 放行、 重定向等多种策略动作）进行规则匹配， 阻断异常流量。

白名单引擎策略设置： 通过自学习模式， 学习和建立正常的流量模型， 后续进行流量比对，而发现异常行为并进行告警和阻断。

3、 部署数量及位置

云平台基础架构的 WEB 应用安全：通过在云平台运维管理区前端部署 2 台硬件 WEB 应用防火墙， 通过双机部署的形式提高可靠性。

互联网区各租户的 WEB 应用安全： 划分独立的服务器资源区，部署虚拟 WEB 应用防火墙， 为每个租户分配 1 套虚拟 WEB 应用防火墙。 通过反向代理的方式将 WEB 流量牵引至虚拟 WEB 应用防火墙上进行过滤后转发给 WEB 服务器。

4、 服务模式

云平台基础架构的 WEB 应用安全： 部署 2 台硬件 WEB 应用防

火墙产品（全局服务）

互联网区各租户的 WEB 应用安全： 每个租户分配 1 套虚拟

WEB 应用防火墙（租户个性化服务）

13.7.5.3 网页防篡改设计

13.7.5.3.1 功能设计

网页防篡改系统包含防篡改、 防攻击两大子系统的多个功能模块， 为网站安全建立全面、 立体的防护体系。 主要功能如下：

1 、 要求采用先进的文件驱动防篡改技术， 实现新一代内核驱动及文件保护，并支持大规模连续篡改攻击保护。

2 、 要 求 支 持 操 作 系 统 ： Windows***0,***3,***8 32&64 位 ；

Redhat,CentOS,SUSE,Asianux 等 32&64 位 ； UNIX 系 列 ：

AIX ,HP-UX,Solaris 。

3 、 要 求 支 持 WEB 服 务 器 ： IIS ， apachejava 系 列 (weblogic,websphere,tomcat,jboss 等) 。

4、 采用先进内核驱动、 WEB 核心内嵌和实时触发机制结合。

5、 支持各类网页文件的保护， 包括静态和动态网页以及各类文件信息。

6、 支持对指定文件夹以及子文件夹的保护， 避免上传非法文件及木马等恶意文件或插入恶意代码。

7、 能够有效防止 SQL 注入攻击、 跨站攻击、 溢出代码攻击、 对危险文件类型的访问、 对危险系统路径的访问、 特殊字符构成的 URL 利用、防止构造危险的 Cookie 等。

13.7.5.3.2 部署设计

1 、 部署条件

根据不同的操作系统平台， 可以选择 Windows、 Linux 、 Unix 对应版本的软件进行安装和使用。

2、 策略设置

在管理控制端上对监控端进行策略配置，添加站点名称、站点文件路径后可添加保护动作（允许修改或阻止修改） 和发布进程路径， 可以保护网站静态文件资源不被恶意篡改。

通过内置规则库和自动义规则， 可以防御 SQL 注入、 XSS 漏洞、 Web Shell 上传检测、 代码注入和特定漏洞的攻击， 保护动态资源安全。

3、 部署数量及位置

监控端独立部署于互联网区各租户的门户网站 / 网站群的 Web 服务器上， 数量取决于 Web 服务器的数量。 管理端和发布端部署于互联网运维管理区。

管理控制端可以安装在任何服务器或 PC 机上， 主要用于配置、 管理和展现监控端、 发布端

的各种信息， 并下发安全规则到监控端。

监控端安装在 WEB 服务器上， 实现对站点进行保护和监测。

同步端安装在 CMS 内容更新服务器上， 实现对站点文件内容实时更新

4、 服务模式

服务模式为租户服务模式， 在网页防篡改管理端上对各租户门户网站服务器上的监控端进行统一的策略管理。

13.7.5.4 网络架构安全

在整个智慧园区大数据云环境中， 要求管理网络系统与业务网络分离，而 xxx 网云平台网络系统和电子政务互联网云平台网络系统之间物理隔离。

13.7.6 数据安全

13.7.6.1 功能设计

数据库审计： 实现细粒度审计、 精准化行为回溯、 全方位风险控制，为核心数据库提供全方位、 细粒度的保护功能， 可帮助用户带来如下价值点：

全面记录数据库访问行为， 识别越权操作等违规行为， 并完成追踪溯源

跟踪敏感数据访问行为轨迹， 建立访问行为模型， 及时发现敏感数据泄漏

检测数据库配置弱点、 发现 SQL 注入等漏洞、 提供解决建议

为数据库安全管理与性能优化提供决策依据

提供符合法律法规的报告， 满足等级保护、 内控等审计要求

13.7.6.2 部署设计

1 ．部署条件

采用旁路模式部署， 通过在接入交换机或网络设备上启用端口镜像功能， 将对数据库的访问和返回流量复制一份到数据库审计产品

上， 从而进行对数据库流量的安全审计。

2. 策略设置

添加保护对象： 需要设置保护对象的 IP 地址、 数据库类型（ Oracle 、SyBase 等）、 数据库版本、 端口号， 运行环境（Linux 、Windows 等） 、 流量方向（单向审计、 双向审计） 。

业务群组绑定多个保护对象： 数据库审计产品需多个业务群组，而每个业务群组内包含多台数据库主机（保护对象） 。

添加审计规则 ： 支持以 IP 来源、 操作类型、 报文关键字时间等条件设置审计规则， 并能以规则组的形式进行添加。

查询审计结果： 支持以对象、 操作类型、 业务主机群、 账号、 客户端 IP、 报文等条件进行筛选查询审计结果。

查询风险告警： 支持以风险级别、 业务主机群、 客户端 IP 、 状态、 规则等条件进行筛选查看风险告警结果。

3. 部署数量及位置

互联网区： 1 台， 旁挂在数据库接入交换机上

xxx 网区： 1 台， 旁挂在数据库接入交换机上

4、 服务模式

本方案中数据库审计产品采用硬件的方式进行部署， 分别为云基础架构的数据库流量提供全局审计， 为租户数据库流量提供全局的审计服务。

13.7.7 管理安全

13.7.7.1 安全管理机构

设立信息安全管理工作的职能部门， 设立安全主管人、 安全管理各个方面的负责人， 定义各负责人的职责；

设立系统管理人员、 网络管理人员、 安全管理人员岗位， 定义各个工作岗位的职责；

成立指导和管理信息安全工作的委员会或领导小组， 其最高领导应由单位主管领导委任或授权；

制定文件明确安全管理机构各个部门和岗位的职责、 分工和技能要求。

配备一定数量的系统管理人员、 网络管理人员和安全管理人员等；

配备专职安全管理人员， 不可兼任；

关键区域或部位的安全管理人员应按照机要人员条件配备；

关键岗位应定期轮岗；

关键事务应配备多人共同管理；

授权审批部门及批准人， 对关键活动进行审批；

列表说明须审批的事项、 审批部门和可批准人；

建立各审批事项的审批程序， 按照审批程序执行审批过程；

建立关键活动的双重审批制度；

不再适用的权限应及时取消授权；

定期审查、 更新需授权和审批的项目；

记录授权过程并保存授权文档；

加强各类管理人员和组织内部机构之间的合作与沟通， 定期或不定期召开协调会议， 共同协

助处理信息安全问题；

信息安全职能部门应定期或不定期召集相关部门和人员召开安全工作会议， 协调安全工作的实施；

信息安全领导小组或者安全管理委员会定期召开例会， 对信息安全工作进行指导、决策；

加强与兄弟单位和公安机关的合作与沟通， 以便在发生安全事件时能够得到及时的支持；

加强与供应商、 业界专家、 专业的安全公司、 安全组织的合作与沟通， 获取信息安全的最新发展动态， 当发生 急事件的时候能够及时得到支持和帮助；

文件说明外联单位、 合作内容和联系方式；

聘请信息安全专家， 作为常年的安全顾问， 指导信息安全建设， 参与安全规划和安全评审等；

由安全管理人员定期进行安全检查， 检查内容包括用户账号情况、 系统漏洞情况、系统审计情况等；

由安全管理部门组织相关人员定期进行全面安全检查， 检查内容包括现有安全技术措施的有效性、 安全配置与安全策略的一致性、 安全管理制度的执行情况等；

由安全管理部门组织相关人员定期分析、 评审异常行为的审计记录， 发现可疑行为，形成审计分析报告， 并采取必要的应对措施；

制定安全检查表格实施安全检查， 汇总安全检查数据， 形成安全检查报告， 并对安全检查结果进行通报；

制定安全审核和安全检查制度规范安全审核和安全检查工作， 定期按照程序进行安全审核和安全检查活动。

13.7.7.2 安全管理制度

制度具有统一的格式风格， 并进行版本控制；

组织相关人员对制定的安全管理进行论证和审定；

安全管理制度应经过管理层签发后按照一定的程序以文件形式发布；

安全管理制度应注明发布范围， 并对收发文进行登记；

安全管理制度应注明密级， 进行密级管理；

定期对安全管理制度进行评审和修订， 对存在不足或需要改进的安全管理制度进行修订；

当发生重大安全事故、 出现新的安全漏洞以及技术基础结构发生变更时， 应对安全管理制度进行检查、 审定和修订；

每个制度文档应有相应负责人或负责部门， 负责对明确需要修订的制度文档的维护；

评审和修订的操作范围应考虑安全管理制度的相应密级。

13.7.7.3 人员安全管理

保证被录用人具备基本的专业技术水平和安全管理知识；

对被录用人声明的身份、 背景、 专业资格和资质等进行审查；

对被录用人所具备的技术技能进行考核；

对被录用人说明其角色和职责；

签署保密协议；

对从事关键岗位的人员应从内部人员选拔， 并定期进行信用审查；

对从事关键岗位的人员应签署岗位安全协议。

立即终止由于各种原因即将离岗的员工的所有访问权限；

取回各种身份证件、 钥匙、 徽章等以及机构提供的软硬件设备；

经机构人事部门办理严格的调离手续， 并承诺调离后的保密义务后方可离开；

关键岗位的人员调离应按照机要人员的有关管理办法进行。

对所有人员实施全面、 严格的安全审查；

定期对各个岗位的人员进行安全技能及安全认知的考核；

对考核结果进行记录并保存；

对违背安全策略和规定的人员进行惩戒。

对各类人员进行安全意识教育；

告知人员相关的安全责任和惩戒措施；

制定安全教育和培训计划， 对信息安全基础知识、 岗位操作规程等进行培训；

针对不同岗位制定不同培训计划；

对安全教育和培训的情况和结果进行记录并归档保存。

13.7.7.4 系统建设管理

13.7.7.4.1 系统定级

明确信息系统划分的方法；

确定信息系统的安全保护等级；

以书面的形式定义确定了安全保护等级的信息系统的属性， 包括使命、 业务、 网络、 硬件、软件、 数据、 边界、 人员等；

以书面的形式说明确定一个信息系统为某个安全保护等级的方法和理由；

组织相关部门和有关安全技术专家对信息系统的定级结果的合理性和正确性进行论证和审定；

确保信息系统的定级结果经过相关部门的批准。

13.7.7.4.2 系统备案

系统定级、 系统属性等材料指定专门的人员或部门负责管理， 并控制这些材料的使用；

系统等级和系统属性等资料报系统主管部门备案；

系统等级、 系统属性、 等级划分理由及其他要求的备案材料报相应公安机关备案。

13.7.7.4.3 安全方案设计

根据系统的安全级别选择基本安全措施， 依据风险评估的结果补充和调整安全措施；

指定和授权专门的部门对信息系统的安全建设进行总体规划， 制定近期和远期的安全建设工作计划；

根据信息系统的等级划分情况， 统一考虑安全保障体系的总体安全策略、 安全技术框架、 安全管理策略、 总体建设规划和详细设计方案， 并形成配套文件；

组织相关部门和有关安全技术专家对总体安全策略、 安全技术框架、 安全管理策略、 总体建设规划、 详细设计方案等相关配套文件的合理性和正确性进行论证和审定；

确保总体安全策略、 安全技术框架、 安全管理策略、 总体建设规划、 详细设计方案等文件必须经过批准， 才能正式实施；

根据安全测评、 安全评估的结果定期调整和修订总体安全策略、 安全技术框架、安全管理策略、 总体建设规划、 详细设计方案等相关配套文件。

13.7.7.4.4 产品采购

确保安全产品的使用符合国家的有关规定；

确保密码产品的使用符合国家密码主管部门的要求；

指定或授权专门的部门负责产品的采购；

制定产品采购方面的管理制度明确说明采购过程的控制方法和人员行为准则；

预先对产品进行选型测试， 确定产品的候选范围， 并定期审定和更新候选产品名单；

13.7.7.4.5 自行软件开发

开发环境与实际运行环境物理分开；

系统开发文档由专人负责保管， 系统开发文档的使用受到控制；

制定开发方面的管理制度明确说明开发过程的控制方法和人员行为准则；

开发人员和测试人员的分离， 测试数据和测试结果受到控制；

提供软件设计的相关文档和使用指南；

13.7.7.4.6 外包软件开发

与软件开发单位签订协议， 明确知识产权的归属和安全方面的要求；

根据协议的要求检测软件质量；

在软件安装之前检测软件包中可能存在的恶意代码；

要求开发单位提供技术培训和服务承诺；

要求开发单位提供软件设计的相关文档和使用指南；

13.7.7.4.7 工程实施

与工程实施单位签订与安全相关的协议， 约束工程实施单位的行为；

指定或授权专门的人员或部门负责工程实施过程的管理；

制定详细的工程实施方案控制实施过程， 并要求工程实施单位能正式地执行安全工程过程；

制定工程实施方面的管理制度明确说明实施过程的控制方法和人员行为准则；

13.7.7.4.8 测试验收

对系统进行安全性测试验收；

在测试验收前根据设计方案或合同要求等制订测试验收方案， 测试验收过程中详细记录测试验收结果， 形成测试验收报告；

委托公正的第三方测试单位对系统进行测试， 并出具测试报告；

制定系统测试验收方面的管理制度明确说明系统测试验收的控制方法和人员行为准则；

指定或授权专门的部门负责系统测试验收的管理， 并按照管理制度的要求完成系统测试验收工作；

组织相关部门和相关人员对系统测试验收报告进行审定， 没有疑问后由双方签字。

13.7.7.4.9 系统交付

明确系统的交接手续， 并按照交接手续完成交接工作；

由系统建设方完成对委托建设方的运维技术人员的培训；

由系统建设方提交系统建设过程中的文档和指导用户进行系统运行维护的文档；

由系统建设方进行服务承诺， 并提交服务承诺书， 确保对系统运行维护的支持；

制定系统交付方面的管理制度明确说明系统交付的控制方法和人员行为准则；

指定或授权专门的部门负责系统交付的管理工作， 并按照管理制度的要求完成系统交付工作。

13.7.7.4.10 安全测评

在系统投入运行前进行安全测评， 测评后符合相应等级保护标准要求的才能投入使用；

在系统运行过程中定期对系统进行安全测评， 发现不符合相应等级保护标准要求的及时整改；

在系统发生变更时及时对系统进行安全测评， 发现级别发生变化的及时调整级别并进行安全改造； 发现不符合相应等级保护标准要求的及时整改；

与测评单位签订与安全相关的协议， 约束测评单位的行为；

指定或授权专门的人员或部门负责安全测评的管理。

13.7.7.5 系统运维管理

13.7.7.5.1 环境管理

对机房供配电、 空调、 温湿度控制等设施指定专人或专门的部门定期进行维护管理；

配备机房安全管理人员， 对机房的出入、 服务器的开机或关机等工作进行管理；

建立机房安全管理制度， 对有关机房物理访问， 物品带进、 带出机房和机房环境安全等方面的管理作出规定；

加强对办公环境的保密性管理， 包括如工作人员调离办公室应立即交还该办公室钥匙和不在办公区接待来访人员等；

对办公环境的人员行为， 如工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件等作出规定；

有指定的部门负责机房安全， 并配置电子门禁系统和专职警卫， 对机房来访人员实行登记记录、 电子记录和监控录像三重备案管理；

13.7.7.5.2 资产管理

建立资产安全管理制度， 规定信息系统资产管理的责任人员或责任部门， 并规范资产管理和使用的行为；

编制并保存与信息系统相关的资产、 资产所属关系、 安全级别和所处位置等信息的资产清单；

根据资产的重要程度对资产进行定性赋值和标识管理， 根据资产的价值选择相应的管理措施；

确定信息分类与标识的原则和方法， 并对信息的使用、 传输和存储作出规定；

13.7.7.5.3 介质管理

建立介质安全管理制度， 对介质的存放环境、 使用、 维护和销毁等方面作出规定；

介质的归档和查询须有记录， 并对存档介质的目录清单定期盘点；

对于需要送出维修或销毁的介质， 应采用多次读写覆盖， 清除介质中的敏感或秘密数据， 防止信息的非法泄漏， 对无法执行删除操作的受损介质必须销毁；

根据数据备份的需要对某些介质实行异地存储， 存储地的环境要求和管理方法应与本地相同；

根据所承载数据和软件的重要程度对介质进行分类和标识管理， 并实行存储环境专人管理；

对介质的物理传输过程中人员选择、 打包、 交付等情况进行控制；

对存储介质的使用过程、 送出维修以及销毁等进行严格的管理， 保密性较高的信息存储介质未经批准不得自行销毁， 销毁时必须做到双人监销， 销毁记录应妥善保存；

重要数据存储在本地或带出工作环境必须采取加密方式存储， 并进行监控管理；

对存放在介质库中的介质定期进行完整性和可用性检查， 确认其数据或软件没有受到损坏或丢失。

13.7.7.5.4 设备管理

对信息系统相关的各种设备、 线路等指定专人或专门的部门定期进行维护管理；

对信息系统的各种软硬件设备的选型、 采购、 发放或领用等过程建立基于申报、审批和专人负责的管理规定；

对终端计算机、 工作站、 便携机、 系统和网络等设备的操作和使用建进行规范化管理；

对带离机房或办公地点的信息处理设备进行控制；

按操作规程实现服务器的启动 / 停止、 加电 / 断电等操作， 加强对服务器操作的日志文件管理和监控管理， 并对其定期进行检查；

建立配套设施、 软硬件维护方面的管理制度， 对其维护进行有效的管理， 包括明确维护人员的责任、 涉外维修和服务的审批、 维修过程的监督控制等；

在安全管理机构统一安全策略下对服务器进行系统配置和服务设定， 并实施配置管理。

13.7.7.5.5 监控管理

进行主机运行监视， 包括监视主机的 CPU、 硬盘、 内存、 网络等资源的使用情况；

对分散或集中的安全管理系统的访问授权、 操作记录、 日志等方面进行有效管理；

严格管理运行过程文档， 其中包括责任书、 授权书、 许可证、 各类策略文档、 事故报告处理文档、 安全配置文档、 系统各类日志等， 并确保文档的完整性和一致性；

13.7.7.5.6 网络安全管理

指定专人对网络进行管理， 负责运行日志、 网络监控记录的日常维护和报警信息分析和处理工作；

根据厂家提供的软件升级版本对网络设备进行更新， 并在更新前对现有的重要文件进行备份；

进行网络系统漏洞扫描， 对发现的网络系统安全漏洞进行及时的修补；

保证所有与外部系统的连接均应得到授权和批准；

建立网络安全管理制度， 对网络安全配置、 网络用户以及日志等方面作出规定；

对网络设备的安全策略、 授权访问、 最小服务、 升级与打补丁、 维护记录、 日志以及配置文件的生成、 备份、 变更审批、 符合性检查等方面做出具体规定；

规定网络审计日志的保存时间以便为可能的安全事件调查提供支持；

明确各类用户的责任、 义务和风险， 并按照机构制定的审查和批准程序建立用户和分配权限，定期检查用户实际权限与分配权限的符合性；

对日志的备份、 授权访问、 处理、 保留时间等方面做出具体规定， 使用统一的网络时间， 以确保日志记录的准确；

通过身份鉴别、 访问控制等严格的规定限制远程管理账户的操作权限和登录行为；

定期检查违反规定拨号上网或其他违反网络安全策略的行为；

13.7.7.5.7 系统安全管理

指定专人对系统进行管理， 删除或者禁用不使用的系统缺省账户；

制定系统安全管理制度， 对系统安全配置、 系统账户以及审计日志等方面作出规定；

对能够使用系统工具的人员及数量进行限制和控制；

定期安装系统的最新补丁程序， 并根据厂家提供的可能危害计算机的漏洞进行及时修补， 并在安装系统补丁前对现有的重要文件进行备份；

根据业务需求和系统安全分析确定系统的访问控制策略， 系统访问控制策略用于控制分配信息系统、 文件及服务的访问权限；

对系统账户进行分类管理， 权限设定应当遵循最小授权要求；

对系统的安全策略、 授权访问、 最小服务、 升级与打补丁、 维护记录、 日志以及配置文件的生成、 备份、 变更审批、 符合性检查等方面做出具体规定；

规定系统审计日志的保存时间以便为可能的安全事件调查提供支持；

进行系统漏洞扫描， 对发现的系统安全漏洞进行及时的修补；

明确各类用户的责任、 义务和风险， 对系统账户的登记造册、 用户名分配、 初始口令分配、用户权限及其审批程序、 系统资源分配、 注销等作出规定；

对于账户安全管理的执行情况进行检查和监督， 定期审计和分析用户账户的使用情况， 对发现的问题和异常情况进行相关处理。

13.7.7.5.8 恶意代码防范管理

提高所用用户的防病毒意识， 告知及时升级防病毒软件；

在读取移动存储设备（如软盘、 移动硬盘、 光盘） 上的数据以及网络上接收文件或邮件之前，先进行病毒检查， 对外来计算机或存储设备接入网络系统之前也要进行病毒检查；

指定专人对网络和主机的进行恶意代码检测并保存检测记录；

对防恶意代码软件的授权使用、 恶意代码库升级、 定期汇报等作出明确管理规定；

定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录， 对主机防病毒产品、 防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理， 并形成书面的报表和总结汇报。

13.7.7.5.9 密码管理

建立密码使用管理制度， 密码算法和密钥的使用应符合国家密码管理规定。

13.7.7.5.10 变更管理

确认系统中要发生的变更， 并制定变更方案；

建立变更管理制度， 重要系统变更前， 管理人员应向主管领导申请， 变更和变更方案经过评审、 审批后方可实施变更；

系统变更情况应向所有相关人员通告；

应建立变更控制的申报和审批文件化程序，变更影响分析应文档化，变更实施过程应记录，所有文档记录应妥善保存；

中止变更并从失败变更中恢复程序应文档化， 应明确过程控制方法和人员职责，必要时恢复过程应经过演练；

13.7.7.5.11 备份与恢复管理

识别需要定期备份的重要业务信息、 系统数据及软件系统等；

规定备份信息的备份方式（如增量备份或全备份等） 、 备份频度（如每日或每周等） 、 存储介质、 保存期等；

根据数据的重要性和数据对系统运行的影响， 制定数据的备份策略和恢复策略，备份策略应指明备份数据的放置场所、 文件命名规则、 介质替换频率和将数据离站运输的方法；

指定相应的负责人定期维护和检查备份及冗余设备的状况，确保需要接入系统时能够正常运行；

建立控制数据备份和恢复过程的程序， 备份过程应记录， 所有文件和记录应妥善保存；

根据系统级备份所采用的方式和产品， 建立备份及冗余设备的安装、 配置、 启动、操作及维护过程控制的程序， 记录设备运行过程状况， 所有文件和记录应妥善保存；

定期执行恢复程序， 检查和测试备份介质的有效性， 确保可以在恢复程序规定的时间内完成备份的恢复；

13.7.7.5.12 安全事件处置

所有用户均有责任报告自己发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点；

制定安全事件报告和处置管理制度， 规定安全事件的现场处理、 事件报告和后期恢复的管理职责；

分析信息系统的类型、 网络连接特点和信息系统用户特点， 了解本系统和同类系统已发生的安全事件， 识别本系统需要防止发生的安全事件， 事件可能来自攻击、错误、 故障、 事故或灾难；

根据国家相关管理部门对计算机安全事件等级划分方法， 根据安全事件在本系统产生的影响，将本系统计算机安全事件进行等级划分；

制定的安全事件报告和响应处理程序， 确定事件的报告流程， 响应和处置的范围、程度， 以及处理方法等；

在安全事件报告和响应处理过程中， 分析和鉴定事件产生的原因，收集证据， 记录处理过程，总结经验教训， 制定防止再次发生的补救措施， 过程形成的所有文件和记录均应妥善保存；

对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序；

13.7.7.5.13 应急预案管理

在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、 系统恢复流程和事后教育和培训等内容；

从人力、 设备、 技术和财务等方面确保应急预案的执行有足够的资源保障；

对系统相关的人员进行培训使之了解如何及何时使用应急预案中的控制手段及恢复策略， 对应急预案的培训至少每年举办一次；

应急预案须定期演练， 根据不同的应急恢复内容， 确定演练的周期；

规定应急预案需要定期审查和根据实际情况更新的内容， 并按照执行。

13.7.8 安全服务

13.7.8.1 安全评测服务

云平台等保三级测评服务：按照信息系统等级保护要求，提供信息系统定级备案、差距测评、安全整改、等保测评全流程服务。

13.7.8.2 安全检测服务

13.7.8.3 系统漏洞检测服务

1、严格按照计算机信息系统安全的国家标准，对不同操作系统下的计算机（在可扫描 IP 范围内）进行漏洞检测。可分析和指出有关网络的安全漏洞及被测系统的薄弱环节，给出详细的检测报告，并针对检测到的网络安全隐患给出相应的修补措施和安全建议。

2、自动统计总体漏洞数量、统计不同操作系统类型的主机数量、统计所有开发端口、可用帐户、列出每一个漏洞所存在的主机、详细描述与修补建议。漏洞详细描述包括：漏洞名称、详述、修补方案、CVE/Bugtraq/CNVD/CNNV 编 D 号评分等。

3、提供直观的风险危害等级图表和风险类型统计图表、漏洞的描述、漏洞的风险级别、加固建议。

13.7.8.4 Web 漏洞检测服务

1、通过丰富的策略包，针对各种 WEB 应用系统以及各种典型的应用漏洞进行检测（如 SQL 注入、Cookie 注入、XPath 注入、LDAP 注入、跨站脚本、代码注入、表单绕过、弱口令、敏感文件和目录、管理后台、敏感数据、第三方软件等）。

2、对各种挂马方式的网页木马进行全自动、高性能、智能化分析，并对网页木马传播的病毒类型做出准确剖析和网页木马宿主做出精确定位。

3、对逻辑漏洞进行检测，如水平操作权限、短信炸弹、转账支付漏洞、重放攻击、垂直权限页面访问测试、垂直操作权限等。

13.7.8.5 配置核查服务

1、由安全专业人员根据评估范围，基于国家信息安全等级保护标准，采用人工检查用表（Checklist）、脚本程序或基线扫描工具对评估目标范围内的网络安全设备、主机系统、数据库、中间件等进行安全基线配置合规检查，并提供安全加固建议。

2、明确设备的用户和口令安全、文件系统安全、远程接入安全、控制台安全等，使设备具备对攻击的较高防御能力。

13.7.8.6 渗透测试服务

在客户授权的情况下， 安全专家在安全可控的范围内， 通过真实模拟黑客行为、 使用工具和分析方法， 对业务系统进行模拟攻击，并结合智能工具扫描结果， 由渗透测试安全专家进行深入的手工测试和漏洞威胁分析，识别工具弱点扫描无法发现的问题。主要分析内容包括逻辑缺陷、上传绕过、 输入输出校验绕过、 数据篡改、 功能绕过、 异常错误等以及其他专项内容测试与分析。

13.7.8.7 安全评估服务

1 ） 资产评估： 采集资产信息， 进行资产分类， 划分资产重要级别，明确评估的范围和重点， 对组织的关键信息资产进行全面梳理， 识别客户资产的重要性。

2） 威胁评估：分析整体的网络拓扑结构安全隐患，清晰自身所面临的威胁及其威胁方式，有针对性地防护。

3） 脆弱性评估： 基于技术方面的安全评估和管理方面管理评估有效发现脆弱性、 验证脆弱性、 分析判断可利用的途径（已有安全措施验证） 和严重程度， 认识自身存在的脆弱性（不足），有目的性的进行补遗整改工作。

4） 风险处置计划： 明确自身整体安全状态， 制定整体安全规划，逐步完善防护能力、 检测能力、 响应能力、 恢复能力， 实现整体安全。

13.7.8.8 重点安全保障服务

提供每年不少于两次的重大安全保障服务， 在网络运营关键时刻给予现场技术保障， 对网络风险给予评估和规避建议， 帮助客户提升网络运维能力， 控制网络运维风险， 规范网络运维流程，优化网络服务管理。

协助客户进行网络基础信息的分析整理； 协助客户快速分析、诊断、 解决故障， 跟踪问题的处理进展， 提供维护建议； 提供日常维护服务总结及汇报。

13.7.8.9 安全培训服务

根据本次项目中所采用的产品和相关技术， 对用户和现场运维人员每年提供不少于 5 天的全面技术培训， 培训前与用户协商培训计划和课程安排， 以保证用户操作人员能够熟练地操作和维护、 测试、 开发等工作。

13.8 容灾备份方案

13.8.1 容灾数据复制技术

根据国家标准《信息安全技术信息系统灾难恢复规范》 中规定的容灾技术实现等级为：

针对不同等级的数据容灾要求， 可以采用不同的容灾数据复制技术， 容灾数据复制技术实现主要分为 6 个层次：

13.8.1.1 存储级数据容灾技术

1） 适用对象及范围

存储级数据容灾技术主要适用于数据中心级的海量数据复制，对远程数据备份的一致性有很高的要求。 该存储技术也能很好的满足多数据中心间灾难恢复策略的要求。 同时也要求用户必需采用支持该功能的磁盘阵列型号， 而这些阵列一般都采用高端阵列。

2） 实现方式

存储级数据容灾技术是先将业务数据整合到企业级存储， 通过存储间的同步 / 异步的方式将数据复制到同城 / 异地中心。 磁盘阵列将磁盘镜像功能的处理负荷从主机转移到智能磁盘控制器—智能存储系统上。基于智能存储的数据复制由智能存储系统自身实现数据的远程复制和同步，即智能存储系统将对本系统中的存储器 I/O 操作日志复制到远端的存储系统中并执行， 保证数据的一致性。 由于在这种方式下， 数据复制软件运行在存储系统内，因此较容易实现主中心和备份中心的操作系统、 数据库、 系统库和目录的实时拷贝维护能力， 一般不会影响主中心主机系统的性能。 如果在系统恢复场所具备了实时数据， 那么就可能做到在灾难发生的同时及时开始应用处理过程的恢复。

另外， 存储级容灾技术要求存储设备自身具有较强的智能管理功能， 需配置相应的容灾备份管理软件， 配置主、 备用系统存储设备间的网络通信专用接口设备和相应的通信通道。

13.8.1.2 卷管理级数据容灾技术

1） 适用对象及范围

将物理存储设备划分为一个或者多个逻辑磁盘卷（ Volume），便于数据的存储规划和管理。 逻辑磁盘卷可以理解为在物理存储设备和操作系统之间增加一个逻辑存储管理层。 基于逻辑磁盘卷的远程数据复制是指根据需要将一个或者多个卷进行远程同步（或者异步） 复制。 该方案的实现通常通过软件来实现， 基本配置包括卷管理软件和远程复制控制管理软件。

基于逻辑磁盘卷的远程数据复制会增加各节点主机的一些处理性能需求， 在主机性能和通信带宽的要求得到满足时， 远程复制效率和数据一致性可以得到保证。

在同时对多个系统进行容灾份的情况下， 可以通过在备份中心磁盘阵列上划分不同的磁盘卷，以对应不同的系统进行复制或镜像处理的方法。 但是该技术会增加主机的负载。

2） 实现方式

操作系统卷复制级数据容灾的实现方式也包括同步和异步两种， 能够将生产中心主机操作系统上的对逻辑卷的 I/O 操作实时或者延时的复制到容灾中心的操作系统上， 写到容灾中心的逻辑卷当中， 实现不同级别的数据级容灾。

由于是操作系统一级进行工作， 如果是独立的卷管理软件就需要在操作系统上安装相应的软件模块， 如果是采用操作系统自带的卷管理功能， 就无需再安装其他的软件模块。

13.8.1.3 虚拟化级数据容灾技术

1） 适用对象及范围

SAN 虚拟化解决方案有助于应对存储管理的挑战。 SAN 虚拟化解决方案被设计为利用到不同厂商存储子系统的连接创建虚拟存储池， 此存储池能帮助客户利用他们未使用的存储容量， 以使他们的业务更加高效和灵活。 SAN 虚拟化解决方案提供存储卷的单一视图， 从而帮助简化存储的管理。

2） 实现方式

基于 SAN 的存储虚拟化同步镜像实现原理如下：

1 ）主机发出 I/O 请求给专门的存储虚拟化控制器。

2）存储虚拟化设备接收到 I/O 请求后， 先在本地磁盘上执行 I/O 操作。

3）同时， 将 I/O 操作通过 路传输到远程对端的存储虚拟化设备上进行。

4）两端 I/O 操作都完成后， 主机的 I/O 请求被回应。

13.8.1.4 数据库级数据容灾技术

1） 适用对象及范围

远程数据库复制对主机的性能有一定影响， 可能增加对磁盘存储容量的需求（包括对 Log 的存储） ， 但系统恢复较简单， 在实时复制方式时数据一致性较好， 所以对于数据一致性要求较高、 数据修改更新频繁的应用可采用基于数据库的数据备份方案。

2） 实现方式

远程数据库复制是由数据库系统软件来实现数据库的远程复制和同步。 在复制过程中， 使用自动冲突检测和解决的手段保证数据一致性不受破坏。 基于数据库的复制方式可分为实时复制、定时复制和存储转发复制。

1）实时复制： 当主中心的数据库内容被修改时， 备份中心的数据库内容实时地被修改， 此种复制方式对网络可靠性要求高。

2）定时复制：当主中心的数据库内容被修改时，备份中心的数据库内容会按照时间间隔，周期性地按照主中心的更新情况进行刷新，时间间隔可长（几天或几个月 ）可短（几分钟或几秒钟）。

3）存储转发复制：当主中心的数据库内容被修改时，主中心的数据库服务器会先将修改操作日志存储于本地，待时机成熟再转发给备份中心。

远程数据库复制的实质是实现主、备用系统的数据库的数据同步（实时或者准实时同步），即将主用系统数据库操作日志实时或者周期性地复制到备用系统数据库中执行，实现二者数据的一致性。

远程数据库复制需配置数据库远程复制管理软件，并具备主、备用系统间的网络通信条件（例如 TCP/IP 通道）。如图远程数据库复制的容灾份方案中主、备系统中的服务器主机类型、存储设备类型可以不一样。对数据库的操作访问基于开放接口时甚至可以实现不同数据库平台之间的互为备份复制，也可以通过网关（ Gateway）的方式实现不同数据库间的备份复制。此外，主、备系统可通过路由器进行互连。

13.8.1.5 应用级数据容灾技术

1） 适用对象及范围

基于应用软件的数据容灾是指由应用软件来实现数据的远程复制和同步，当主中心失效时，容灾中心的应用软件系统恢复运行，接管主中心的业务。

这种技术是通过在应用软件内部，连接两个异地数据副本，每次的业务处理数据分别存入主中心和备份中心的数据副本中。

但这种方式需要对现有应用软件系统作比较大的修改升级，甚至重新开发，增加应用软件的复杂性，对应用软件开发上技术水平要求较高，系统实施难度大，而且后期维护比较复杂。并且由应用软件来实现数据的复制和同步会对整个业务系统的性能造成较大的影响。

2） 实现方式

应用级数据容灾技术的实现一般是依赖于在应用程序层面对日志的操作，针对应用程序的每一个 transaction 进行分析，将对本地生产数据的修改复制同步到远程容灾中心。这与数据库和中间件的实现方式有很大类似之处。

13.8.2 容灾整体方案架构

（1） 政府主生产中心业务及数据：通过数据备份系统将政府主生产中心存量业务数据按照数据备份策略，通过 IP 线路备份到 A 数据中心。

（2） A 数据中心业务及数据：将运行在 A 数据中心的非关键业务数据通过数据备份系统将数据备份到 B 数据中心；将关键业务应用系统及数据通过存储复制方式备份到 B 数据中心。

（3） B 数据中心业务及数据：将运行在 B 数据中心的非关键业务数据通过数据备份系统将

数据备份到 A 数据中心； 将关键业务应用系统及数据通过存储复制方式备份到 A 数据中心。

（4） 异地灾备中心： 将分别运行在政府主生产中心、 A 数据中心和 B 数据中心非关键业务数据通过数据备份系统备份到异地灾备中心； 将分别运行在 A 数据中心和 B 数据中心关键业务数据通过存储复制的方式备份到异地灾备中心。

13.8.2.1 数据备份

在市级各个单位将其业务应用系统迁移到云平台后， 其各个单位自身本地依然会有一些数据需要进行备份， 而备份的目标位置可以是市政府自身的云平台上， 或者是云服务商云平台上和市异地灾备中心。

无论将数据备份到什么位置， 为了简化管理， 简化操作， 建议采用统一的数据备份接口， 提高数据备份实现效率和提高用户体验。

云数据中心数据备份面临的问题：

随着市级各个单位将应用、 数据等不断向智慧园区大数据云平台上迁移， 同时在智慧园区大数据云数据中心还会保留部分物理架构 IT 系统， 使得这种物理 &云计算混杂架构的环境下数据保护成为智慧园区大数据云运营过程中需要解决的问题。 例如：

业务受到严重影响： 物理环境下的保护方案直接用于云计算环境， 资源争用的问题严重。

可管理性非常差： 物理、 云计算两套保护方案， 无法实现统一、 高效管理。

整体成本高昂： 在物理环境保护方案之外重新部署云计算保护方案， 整体部署成本昂贵。

需要有多种保护方案： 针对于不同等级的业务系统， 应对于不同的 RPO、RTO 要求， 需要有不同等级的保护方案分类保护

混合架构备份：

1） 价值：

降低投入成本： 物理环境和虚拟环境的保护合二为一， 统一的 App、Database 、 Server 、 Storage 保护， 多种级别保护效果， 用一套整体解决方案成本更低；

灵活的系统扩展性： 根据数据中心的规模情况和数据量情况， 对备份系统进行灵活配置和扩展；

全面提升数据安全等级： 广泛的系统平台、 数据库应用及环境、 虚拟化平台兼容性支持， 针对不同重要等级的系统采用合适的数据保护策略， 全面提升数据中心数据安全级别；

统一管理： 物理机和虚拟化平台统一备份管理， 异构存储系统统一快照管理， 本地和异地灾备系统及数据的统一管理， 降低数据中心数据保护的复杂性

2） 亮点：

虚拟环境和物理环境在同一个平台统一管理。 可根据不同环境制定不同的备份策略， 智能的对数据进行保护。

全面优化的虚拟化平台备份， 大幅提升备份效率， 减少恢复时间可达 99%。

高效大数据量保护， 最多可消除 95%重复数据， 支持应用级备份和恢复，更小的恢复细粒度，保证大量应用集中情况下的保护效率。

与 AnyStorage 整合， 提供更为高效和全面的数据保护， 保证服务质量。

13.8.2.2 容灾备份

对于云计算环境下的容灾方案， 需要兼顾 IT 的云计算架构特点和传统物理架构特点， 这样才能实现对这种混合 IT 架构下的应用和数据容灾。

依据不同单位不同业务需求， xxx 采用三种不同的数据复制技术来灵活的实现云计算数据中心环境下的容灾。

数据库复制服务：

在智慧园区大数据云平台上， 提供数据库复制服务。 市级各个单位可以依据自身业务实际容灾需求， 在云平台线上采购数据库复制服务， 云服务运维团队将以线下方式进行服务交付， 并向服务采购单位交付服务测试结果及持续监控报告。

云主机复制服务：

在智慧园区大数据云平台上， 提供云主机复制服务。 市级各个单位可以依据自身业务实际容灾需求， 在云平台线上采购云主机复制服务， 云服务运维团队将以线下方式进行服务交付， 并向服务采购单位交付服务测试结果及持续监控报告。

存储复制服务：

在智慧园区大数据云平台上， 提供云存储复制服务。 市级各个单位可以依据自身业务实际容灾需求， 在云平台线上采购云存储复制服务， 云服务运维团队将以线下方式进行服务交付， 并向服务采购单位交付服务测试结果及持续监控报告。

13.8.2.3 容灾方案配置

灵活、 有效的容灾方案， 需要一定的成本投入， 而对于采用不同的备份方式， 不同的容灾备份数据复制技术， 都会影响最终的容灾建设成本。

13.8.2.4 本地备份方案

本地备份系统是保证 XX 市智慧园区大数据云平台资源池数据安全性的基础， 备份系统能够防止由于逻辑错误造成的数据丢失。 为维护云业务数据的安全， 需要考虑在日常工作中对业务数据进行备份。 备份数据涉及操作系统、 业务数据和虚拟机映像文件三方面。 数据的安全性和可靠性成为了系统建设的核心问题。

云平台资源池在备份管理、 设备利用率、 数据保护策略等方面需要进行统一规划与设计， 针

对备份的不同需求， 需要一套全面、 高效的数据备份恢复系统来保障业务系统安全可靠运行， 实现备份系统的统一管理、 维护， 达到备份架构统一、 集中管理、节约成本的目的。

需要根据数据的特点采用不同的备份方式、 备份恢复策略，对于核心的数据， 要求进行快速备份和恢复， 从而对生产系统的影响减到最小。 对于其他类型的数据需要尽量减少对生产系统的干扰， 构建高效可靠、 技术先进的数据备份系统， 实现业务数据的安全保护。

13.8.2.5 同城灾备方案

分二步实现 XX 市智慧园区大数据云平台系统的同城灾备方案：

1）第一步实现数据级容灾， 在灾备中心新配置 1 台和生产中心同厂商的存储设备， 利用存储设备自带的存储数据复制功能， 实现数据级容灾； 为了保证数据库数据的一致性，建议采用数据库复制技术保证主备中心数据库的数据复制。

2）第二步实现应用级容灾。 在容灾中心配置相应的服务器池连接容灾存储。 当灾难发生或进行灾难恢复演练时，停止容灾复制关系后，容灾中心服务器可以访问容灾中心存储并接管生产。制定接管计划， 包括人员支持， 网络支持，恢复计划， 演练计划等， 建立完善的全人工干预接管机制。

13.8.2.6 异地灾备方案

13.8.2.6.1 关键业务数据灾备方案

对于异地灾备来说， 可以采用 Asynchronous Periodic （异步周期性）模式来实现关键业务数据保护， 这个模式在最小化数据丢失量、 专线带宽消耗和和成本投资等多方面达到一致的平衡点。

提供最佳的磁盘和带宽利用率， 是在任意距离上进行经济高效复制的理想模式。

该模式能够进行远程站点数据的持续即时复制， 并利用 3PAR 快照技术捕捉和镜像最新更新的数据至远程站点。 在快照技术的基础上， 这种非中断即时同步模式的周期通常为 15 分钟（远远小于本次项目中要求的一天备份一次的要求） 。

该系统并非真正地在进行快照时拷贝或复制数据， 而是使用映射结构简单地将快照空间映射至主卷。 只要快照卷中的指定数据块与基础卷中的相同， 它就不会真正消耗磁盘空间。 当数据块被修改后， 只有修改部分的数据块消耗磁盘空间。

对于每个预定的 Asynchronous Periodic （异步周期） 快照， 只有增量 数据才被捕捉并拷贝至远程站点， 实现每次的快速再 同步和低网络带宽消耗。

Asynchronous Periodic Mode （异步周期性模式） 通 过与指定时间点并发的连贯组数据来确

保数据的一致性。 Remote Copy（远程复制） 使用户能够按自身喜 好灵活地定义这些连贯组—小的、 大的甚至组群性 的， 这些组能够从多主机或应用或两者中捕捉虚拟 卷。 此功能还让用户能够粒度地控制即时更新发生的时间和频率， 对那些针对那些网络带宽有限或需要远 程卷同步存在时间间隔的企业客户而言， 显得尤其宝贵。

复制过程：

1） 启动复制： 复制一旦开始， 该模式就会在主 站点创建一个初始的写时复制快照（“快照 A” ） ， 并与指定时间点同步。 该快照作为源 卷， 复制到远程站点。

快照 A 此刻成为下一 次再同步的基础。

2） 再同步： 在主站点创建最新的主卷快照（“快 照 B” ） ， 同时在远程站点（与“快照 A ” 保 持一致） 创建“快照远程 A ” ， 确保随时可 用 的 数 据 副本 在 远 程 站 点 始 终 可 用 。 快 照 A 与 B 相比较后， 只有变化的增量数据被传 输。

3） 完成时： 一经核实远程站点存储最新和一致 的数据副本， 通过删除快照 A 和快照远程 A 来完成再同步周期。 快照 B 此刻将成为下一 次再同步的新基础。

13.8.2.7 数据库备份

13.8.2.7.1 数据库逻辑备份

所谓数据库逻辑备份，就是采用数据库所提供的导出功能将数据库的结构和数据导出为一个或多个文件。 如 MySql 的 mysqldump， SQL Server 的备份维护计划， Oracle 数据库的 expdp，RMAN 备份等。 这种备份方案也是数据级别的备份。 RPO 和 RTO 较长。

对数据库每天进行一次逻辑备份， 生成一个备份文件， 存放在服务器外挂的存储上。 利用备份文件， 可以创建测试环境库， 或者临时数据库。 也可以导入到待恢复数据库里面实现数据库恢复。

13.8.2.7.2 数据库热备 - 集群方案

为了实现数据库系统高可用的要求， 防范服务器硬件故障导致的长时间业务中断， 云数据库提供集群方案来实现热备（如 Oracle RAC 集群） 。

Oracle 集群（ RAC）

RAC（ real application clusters ） ， 是 Oracle 数据库中采用的一项高可用技术， 其逻辑示意图如下图。 Oracle RAC 集群不同于 MySQ，L 是 ShareEverything 架构， 即所有节点共享内存和存储。 RAC 也不同于 SQL SERVE，R 它的所有节点均处于活动状态， 可以均衡负载， 也能提供故障容错和无缝切换功能，将硬件和软件错误造成的影响最小化。

13.8.2.7.3 数据库复制

集群热备方案保障了单节点故障情况下可以自动快速恢复服务。但是如果数据库软件或者共享存储发生故障时， 数据库系统将不可用。 如果发生数据库损坏，此时恢复服务只能依赖前述的数据备份， 这将使得业务遭受较长的停机时间 （几小时甚至几天） ， 以及较长的数据丢失（几小时） 。 如果需要快速的恢复服务，则需要数据库复制技术来进行弥补。

Oracle 数据库复制技术是， 当 Master 生产库发生改变时， 数据库会将数据发生的变化记录成日志文件， 并将日志文件传送到备份库 Slave 上。Slave 库再将主库发生的变化按序应用。 由于这种复制可以是实时发生的， 所以数据丢失的时长可以控制在较短的时间内， 甚至完全不丢失。当 Master 故障时， 可以通过手工切换的方式快速实现服务的恢复。

Oracle DataGuard

Oracle DataGuard 是 Oracle 自带的数据同步功能， 基本原理是将日志文件从原数据库传输到目标数据库， 然后在目标数据库上应用这些日志文件， 从而使目标数据库与源数据库保持同步，是一种数据库级别的高可用性方案。Primary 数据库可以是单实例数据库，也可以是 RAC。Standby 数据库同样即可以是单实例数据库， 也可以是 RAC 结构。

使用 Data Guard ， 管理员能通过将资源密集的备份、 报表总结、 查询等操作转移到 standby 备份库上， 从而减少了主数据库用于执行这些任务所需的工作负载， 提高生产数据库的性能。

13.8.2.8 备份策略

1） 对于云主机默认提供虚拟机级别的备份服务， 云主机高可用需在用户的需求下提供。

2） 对于云数据库默认提供逻辑备份。 数据库热备和数据库复制需在用户的需求下提供。

13.8.3 数据容灾备份方案

13.8.3.1 数据级容灾备份方案

13.8.3.1.1 一般数据备份技术架构

在 XX 智慧园区大数据云中， 数据库区域和业务系统区域各自使用了独立的存储系统， 对于备份要求较低的业务应用系统及数据可以采用集中式备份系统进行备份，将数据库系统区域和业务系统区域的数据备份到同城灾备中心的分布式存储系统中。

1 ） 支持多种模式：

支持一对一、 一对多、 多对一三种模式；

2） 支持重复数据删除：

可以减少数据传输量， 提升传输效率， 有效利用专线带宽， 有效节省存储空间。

3） 恢复方式：

直接恢复至本地介质服务器

直接恢复到本地或者异地的生产环境

4） 特点：

融合： 物理、 虚拟、 云端数据融合保护

统一： 本地、 异地、 多分支机构统一覆盖

完整： 结构化数据与非结构化数据完整保护

SLA： 私有云、 混合云业务连续性保障

管理： 统一运维

13.8.3.1.2 关键数据备份技术架构

在 XX 智慧园区大数据云中， 对于关键业务数据可以借助于存储系统的数据复制功能实现数据容灾， 将数据从生产中心备份到同城灾备中心。

对于有些业务特殊需求的业务系统数据， 也可以通过数据库自身的数据复制技术将数据从生产中心复制到灾备中心。

这样的数据复制架构设计， 可以保证容灾中心数据的可靠性和可用性， 同时简化运维管理操作， 降低运维管理成本。

13.8.3.2 应用级主备灾备方案

13.8.3.2.1 虚拟化平台容灾技术架构

1 ） 重要组件说明

（1） SRA（Storage Replication Array ）

SRA 是存储与 CAS SRM 配合实现异地容灾特性的关键组件，SRA 是存储系统与 SRM 通信的桥梁，当 SRM 创建、 测试、 执行灾难恢复计划时，SRA 将使存储系统密切配合 SRM， 促使这一系列流程的完成。 利用此组件可以实现对存储系统的管理， 它为 SRM 提供存储系统信息， 包括存储系统发现、 复制 LUN 发现、 故障切换测试、 灾难恢复等， 当 SRM 创建、 测试、 恢复恢复计划时，可以立即为 SRM 提供相应资源， 配合 SRM 自动完成虚拟环境的无中断测试、 站点恢复自动化和迁移流程自动化等。

SRA 在各种容灾场景的主要功能：

SRM 创建灾难恢复计划：

SRA 将向 SRM 提供底层存储系统的相关信息， 包括阵列名称、 系统类型、 LUN 信息等， 协助 SRM 创建恢复计划。

SRM 测试灾难恢复计划：

SRA 接受来自 SRM 的故障测试命令， 并将其传递给存储系统， 此时， 恢复站点的存储系统将随即自动产生一个处于激活状态的数据快照，测试恢复站点的数据正确性和可用性。

SRM 执行灾难恢复计划：

SRA 接受来自 SRM 的故障恢复命令， 并将其传递给存储系统， 此时， 存储于恢复站点存储系统的 LUN 副本内的数据存储组将立即启用， 确保恢复站点虚拟机的正常启动。

（2） 存储复制

存储同步复制： 存储阵列一般都支持同步复制功能， 异构的存储阵列也可以通过存储虚拟化网关的同步复制功能， 能够保证远端灾备中心的数据和本地中心的数据保持一致。 同步复制的原理是：

（ 1） 每一个 I/O 写操作都需要等待远程复制完成后才释放。

（ 2） 在进行下一次写操作之前， 本地卷和远程卷都必须完成上次写操作

（ 3） 在返回确认信息之前， 必须等待本地卷和远程卷的 I/O 响应

有最高级别的数据完整性，但可能会因为在阵列之间传送数据的延迟导致应用性能的降低，而且同步复制方式有距离的要求。

同步复制方式说明图

存储异步远程复制： 阵列异步复制， 存储阵列一般都支持异步复制功能， 异步复制方式一般都是周期性进行的， 不能保证本地数据与远端数据的一致， 异步复制的原理是：

（ 1） 在返回确认信息之前， 只需要等待第一个 I/O 响应， 而不必等待本地卷和远程卷同时完成本次操作

（ 2） 这种模式可以处理比同步模式更多的 I/O 请求这种方法提供了比较高的应用性能， 但如果灾难发生， 就会有丢失一些在远程卷上还未更新的数据

13.8.3.2.2 虚拟化平台容灾实现

CAS SRM 的容灾业务是通过在虚拟化管理平台上创建虚拟机保护组， 虚拟机的数据通过存储的复制功能， 在远端存储上保有一份虚拟机的数据， 并通过制定恢复计划来保证受保护虚拟机在特定的恢复流程指导下完成在远端站点的业务恢复。

1） 站点（本地站点和远端站点）

对于异地容灾方式， 可以将数据中心称之为站点， 站点可以分为本地（生产） 站点和远端（灾备） 站点， 通常情况下， 本地站点是需要被保护的站点， 管理生产资源下的业务； 远端站点是用来恢复业务的目标站点， 管理灾备的资源。 如果发生灾难， 本地的业务会恢复到 远端灾备站

点的资源上。 在进行站点容灾配置时需要指定本地站点和远端站点的信息。

2） 资源映射

资源映射用于在站点容灾配置时， 将本地站点受保护虚拟机使用的资源和远端站点的资源建立对应关系， 以便在恢复时 自动进行资源替换， 可以创建的资源映射包括主机池映射、 网络（虚拟交换机和网络策略模版） 映射、 存储（具有复制关系） 映射等。 在发生故障恢复时， 虚拟机将在远端的灾备站点根据资源映射指定的目标属性进行恢复。

3） 保护组

保护组是需要受保护虚拟机的集合， 通过建立保护组， 将同一个数据存储或多个 1 对 1 的关系阵列（对应存储设备的 LUN） 中的虚拟机划分到一个保护组中， 以便统一制定保护策略对虚拟机进行保护，保证保护组中的虚拟机在故障恢复后数据的完整性和一致性。 通过阵列的复制功能将本地存储设备上的数据复制到远端的存储设备， 来保证虚拟机的数据得到保护， 要保证每个虚拟机共享文件系统的 LUN 都处于同一个阵列。 这样才能达到虚拟机所有磁盘受保护。

4） 恢复计划

指定了一组标准动作， 执行恢复计划时， 指定的标准动作将在保护策略上执行。 在灾难发生后， 将按照恢复计划中指定的动作， 把恢复策略对应的保护组中的虚拟机在远端站点恢复起来。

5） 执行恢复计划

恢复计划有四种执行方式， 分别为： 故障演练， 用于测试站点容灾配置的正确与否； 计划恢复， 一般用于较长时间的保护站点维护；

故障恢复， 保护站点由于各种原因崩溃毁坏时使用； 反向恢复， 计划恢复后或故障恢复后，保护站点恢复正常时使用， 将受保护虚拟机在保护站点恢复。

13.8.3.2.3 业务容灾实现流程

（ 1） 站点配置管理： 容灾方案包括本地站点和远端站点， 由于两个站点的地域跨度比较远，因此通过统一的一个管理平台实现两个站点之间的匹配， 并且通过增加存储适配器来获取两个站点的存储阵列上具有复制关系的卷的对应关系， 以此实现存储的资源映射。

（ 2） 保护组管理： 在本地站点上创建保护组， 将需要保护的虚拟机放入特定的保护组中，由于存储阵列的复制最小单位是 LUN， 因此， 对于已经配置了复制关系的 LUN 上面放置的虚拟机的数据都会复制到远端站点的存储阵列上。

（ 3） 恢复计划管理： 不同的保护组有不同的恢复策略， 恢复计划就是针对不同保护组设置不同的故障恢复策略， 使得本地站点的虚拟机按照特定的策略在远端站点正常启动。

（ 4） 一键故障恢复： 故障恢复包含有多个使用场景， 故障演练场景是在不影响本地虚拟机业务的情况下， 通过将远端站点存储数据的快照进行挂载来模拟故障的发生， 依此来验证恢复计划的正确性，演练完毕后需要通过终止演练来实现演练场景的环境清理； 计划故障恢复场景一般用于数据中心维护的情况， 有计划的故障恢复可以做到正常的关闭虚拟机， 并通过手动触发方式将

关机后的存储最终再做一次数据同步， 能够做到数据不丢失， 然后再进行故障恢复的流程； 故 障恢复场景则是真正的灾难发生时， 将本地虚拟机业务在远端恢复起来的过程， 对于异步复制， 会存在部分数据的丢失； 故障反向恢复场景则是当本地站点故障后， 切换到远端灾备站点， 当原来的本地环境恢复后， 又切换回原来本地的场景。

上述过程都是通过 CAS 的 CVM 管理平台进行管理和配置的， 管理员针对权限范围内的设备进行管理。

13.8.3.2.4 数据库系统容灾技术架构

在 XX 智慧园区大数据云中， 数据库区域、 业务系统区域和互联网业务系统区域各自使用了独立的存储系统， 每个区域的存储系统都是统一厂商统一型号产品， 对于关键业务数据可以借助于存储系统的数据复制功能实现备份。

在灾备数据中心同样部署一套同系列的存储系统， 增加存储系统磁盘容量， 通过在存储复制功能将物理架构下的关键业务数据复制到灾备中心。

当前数据中心双活建设方案源自容灾建设的需求， 最终容灾建设模式从同城灾备中心容灾建设，到两地三中心容灾建设， 在两地三中心建设前期， 为了提到容灾能力， 一般采用大异地， 小同城； 而后来转变为大同城小异地。

当开始建设大同城数据中心后， 需求由原来的 粹作为生产中心的备份， 转变为能够提供部分生产业务的生产中心， 首先这样的转变在于用户对业务可持续服务能力的需求提高， 其次， 是为了有效提高 IT 投资效益。

在市场上双活方案分为以下两类：

资源型双活中心： 主要包含在同城的两个数据中心实现“网络双活”、“计算双活” 和“存储双活” 。 而市场中， 厂家推出的方案最多的是基于存储的双活。

优点： 可以有效必满因为物理设备故障、 电力故障和其它灾难造成系统不可用时， 最小化降低业务不可用时间， 也就是指在容灾指标中的 RTO 可以控制几个小时内或者更短。

缺点： 资源双活相对于主备并没有给用户带来实质性的价值； 如果要产生价值需要应用软件和系统软件的配合才可以， 并且投资巨大。

业务性双活中心： 主要包含数据库双活、 业务应用双活和业务双活； 三者的区别在于数据库双活和业务应用双活都可以独立实现； 而业务双活依赖于数据库双活和业务应用双活同时的实现，而业务双活是双活数据中心建设的最为理想的方案， 但是当前实现困难很大， 而且需要用户巨额投资。

优点： 可以有效必满因为物理设备故障、 电力故障和其它灾难造成系统不可用时， 最小化降低业务不可用时间， 也就是指在容灾指标中的 RTO 可以控制几个小时内或者更短； 数据可用性更高。

缺点： 投资巨大， 维护费用高对维护人员能力要求高。

总结：

数据中心双活方案用户所面临的相同的特点是投资高， 运维难度大，运维人员要求高； 还有一个不被关注的问题是， 双活方案无法对数据逻辑错误提供保护。 例如， 数据误删除， 双活方案无法解决。

所以为了应对数据逻辑错误， 在双活方案建设中， 必须对关键业务系统数据多容灾备份， 采用合理的容灾备份技术手段， 来规避数据逻辑错误。

13.8.3.2.5 分布式存储容灾实现设计

分布式存储系统 A、 B 中心间容灾的实现：

xxxOneStore 分布式存储系统支持基于存储块级别的数据复制功能，对于部署在分布式存储上的重要业务系统及数据， 可以通过此方式将数据从 A 数据中心容灾到 B 数据中心。

OneStore 分布式存储系统容灾功能特点：

基于快照差异的容灾技术， 实现存储级容灾，

利用代理机制和应用联动， 保证数据库数据一致性，

分布式容灾机制， 不存在单点故障，

网络容错， 支持断点续传，

支持容灾策略设置。

分布式存储系统 A 和 B 中心到异地灾备中心容灾的实现：

对于非关键业务系统， 通过数据备份系统将数据从 A、 B 数据中心将数据直接备份到异地灾备中心， 备份策略可以依据业务需要进行灵活制定。

备份到异地灾备中心的数据， 可以实现在异地数据中心进行快速恢复， 并通过异地灾备中心本地的验证主机系统， 实现数据有效性验证，从而确保数据的可用性。

13.8.3.3 XX 智慧园区大数据云备份方案

在 XX 智慧园区大数据云双中心架构设计中， 生产中心 1 和生产中心 2 采用了相同的 IT 架构， 充分考虑了容灾的实现与管理需求，既能够实现生产中心整体切换， 又能实现生产中局部故障造成的部分切换。 在考虑 IT 架构容灾需求的同时， 也重点考虑的业务应用及数据备份的需求，所以， 在两个生产中心均部署了分布式存储系统和数据备份系统， 对生产中心的业务应用和数据进行备份。

为实现两个生产中心之间业务的互备， 网络架构设计如下所示：

为实现对 A、 B 两个生产中心数据级备份， 生产机房和同城灾备机房通过一根千兆 Mb 的 IP 线路互联， 生产中心存储和同城数据中心存储之间的数据异步复制通过此网络进行

13.9 云管理平台相关接口及功能

通过云管理平台相关接口， 实现对不同计算资源， 存储资源， 网络资源的统一管理。

13.9.1 云管理平台 API 清单

13.9.1.1 用户管理

查询用户信息列表

查询用户信息

增加用户

修改用户

删除用户

查询用户附件信息定义列表

查询用户附加信息定义

增加用户附加信息定义

修改用户附加信息定义

删除用户附加信息定义

查询自助账户所有的权限信息列表

查询自助账户名称

查询群组信息列表

查询群组信息

增加群组

修改群组

删除群组

13.9.1.2 网络故障管理

查询告警信息列表

查询告警信息

查询根源告警信息

查询子告警信息列表

查询告警 TopN 设备列表

查询告警用户信息列表

查询告警事件信息列表

查询告警分类列表

查询告警级别列表

查询告警来源类型列表

查询告警恢复状态列表

查询告警确认状态列表

查询告警时间范围列表

恢复告警

确认告警

删除告警

注册告警服务器推送事件

13.9.1.3 网络性能管理

查询摘要列表

查询指标组列表

查询性能指标列表

查询单设备单指标实例列表

查询单指标多设备性能汇总数据列表

查询单指标单接口性能数据

查询单实例性能明细数据

查询单指标 TopN 数据列表

增加自定义性能指标

删除自定义性能指标

修改全局阈值

13.9.1.4 服务运维管理

查询流程模板信息列表

查询流程模板信息

按标识信息及版本信息查询流程模板信息

查询流程信息列表

查询流程信息

根据流程 ID 查询流程的管理权限信息根

据流程 ID 查询流程的任务权限信息根据

流程名和流程模板 ID 查询流程信息

根据流程模板 ID 查询属于此模板的流程信息

创建流程实例

查询流程实例

V3.0 智慧工业园区大数据云平台建设方案

第 729 页

根据流程实例执行 ID 查询流程实例的当前任务信息

执行流程实例

查询知识库 / 问题库分类信息列表

查询知识库 / 问题库分类信息

增加知识库 / 问题库分类信息

删除知识库 / 问题库分类信息

查询知识库信息

增加知识库信息

查询问题库信息

增加问题库信息

13.9.1.5 云业务管理

创建主机

修改主机

删除主机

查看主机

查看主机列表

启动主机

主机重启

关闭主机

加载硬盘

卸载硬盘

创建硬盘

销毁硬盘

查看硬盘列表

创建负载均衡器

删除负载均衡器

查看负载均衡器

查看负载均衡器列表

配置监听器

配置后端服务

删除监听器

查看监听器列表

创建数据库实例

删除数据库实例

修改数据库实例

查看实例列表

启动数据库实例

停止数据库实例

修改数据库配置

查看数据库实例

查看系统镜像

查看自定义镜像

创建自定义镜像

删除自定义镜像

查看工单列表

创建工单

回复工单

删除工单

申请存储

删除云存储

修改存储

查看存储列表

查看存储

查看费用列表

查看主机消费列表

查看硬盘消费列表

查看存储消费列表

查看数据库消费列表

查看负载均衡消费列表

查看防火墙消费列表

查看操作日志列表

查看防火墙

查看网络列表

查看主机类型列表

13.9.2 虚拟化 API 清单

13.9.2.1 主机管理

查询所有主机

查询主机详细信息

查询主机所有虚拟机

查询主机所有虚拟机的 cpu 利用率

查询主机所有虚拟机的内存利用率

查询主机所有虚拟机的 IO 吞吐量

查询主机所有虚拟机的网络吞吐量

查询主机所有共享存储

查询指定虚拟交换机虚拟口信息

查询主机所有虚拟交换机

查询主机某一个虚拟交换机信息

创建虚拟交换机

修改虚拟交换机

删除虚拟交换机

13.9.2.2 虚拟机管理

创建虚拟机

启动虚拟机

正常关闭虚拟机

关闭虚拟机电源

暂停虚拟机

恢复虚拟机

重启虚拟机

休眠虚拟机

删除虚拟机

查询虚拟机详细信息

查询虚拟机网络信息

查询虚拟机快照信息

创建虚拟机快照

删除虚拟机快照

从快照还原

迁移虚拟机

修改虚拟机基本信息

修改虚拟机 CPU 配置

修改虚拟机内存配置

修改虚拟机引导设备配置

修改虚拟机存储配置

修改虚拟机网络配置

修改虚拟机 VNC 配置

修改虚拟机显卡配置

断开虚拟机光驱

连接虚拟机光驱

虚拟机添加虚拟硬盘

卸载虚拟机虚拟硬盘

修改虚拟机网卡连接

删除虚拟机网卡连接

虚拟机名称重名检测

克隆虚拟机

批量部署虚拟机

备份虚拟机

查询 VNC 配置参数

13.9.2.3 虚拟机模板管理

查询虚拟机模板列表

增加虚拟机模板

删除虚拟机模板

13.9.2.4 存储管理

查询存储池列表

查询存储卷列表

增加存储卷

删除存储卷

13.9.2.5 网络策略模板管理

查询网路策略模板列表

查询指定网络策略模板信息

增加网络策略模板

修改网络策略模板

删除网络策略模板

13.9.2.6 告警管理

查询告警信息列表

确认告警信息

删除告警信息

查询告警详细信息

13.9.2.7 任务消息管理

查看任务详细信息

13.9.3 SDN 控制器 API 清单

13.9.3.1 认证管理

生成 Token

删除 Token

13.9.3.2 诊断日志

查询诊断日志开关

修改诊断日志开关

13.9.3.3 操作日志

查询操作日志

13.9.3.4 系统日志

查询系统日志

查询所有监听器

查询指定监听器

增加监听器

修改监听器

删除监听器

13.9.3.5 集群

查询集群

创建集群

修改集群

删除集群

动态加入集群

修改集群成员

动态退出集群

13.9.3.6 Region

13.9.3.

查询所有 Region

查询指定 Region

创建 Region

修改 Region

删除 Region

13.9.3.7 系统信息

查询指定 IP 的系统信息

查询指定 ID 的系统信息

修改控制器 IP 地址

13.9.3.8 组件配置

查询所有组件配置

查询指定组件配置

修改指定组件配置

组件配置恢复默认

13.9.3.9 用户配置

查询用户

增加用户

修改用户密码

删除用户

13.9.3.10 免认证管理

查询免认证用户

增加免认证用户

删除免认证用户

13.9.3.11 统计

查询报文统计信息

查询端口统计信息

查询 Meter 表项统计信息

查询组表项统计信息

查询网络流量统计信息

13.9.3.12 应用程序管理

查询应用程序信息

查询应用程序状态

查询指定应用程序的完整信息

加载应用程序

卸载应用程序

安装应用程序

暂停应用程序

启动应用程序

13.9.3.13 支持报告

查询所有模块的支持报告

13.9.3.14 路管理

查询 路状态信息

13.9.3.15 拓扑时间戳

查询拓扑变化的实时时间戳

13.9.3.16 连通性检测

连通性检测

13.9.3.17 设备管理

查询所有网络设备

查询指定网络设备

查询网络设备所有端口

查询网络设备指定端口

配置网络设备指定端口状态

查询网络设备控制器

查询网络设备 Match 项能力集

查询网络设备流表

下发网络设备流表项

更新网络设备流表项

删除网络设备流表项

查询网络设备组表能力集

查询网络设备所有组表项

查询网络设备指定组表项

下发网络设备组表项

更新网络设备组表项

删除网络设备组表项

查询网络设备 Meter 表能力集

查询网络设备所有 Meter 表项

查询网络设备指定 Meter 表项

下发网络设备 Meter 表项

更新网络设备 Meter 表项

删除网络设备 Meter 表项

13.10 云监管平台

13.10.1 资源监管

资源监管是云监管平台的核心功能之一， 主要目的是对云服务商的各类资源配置情况、 运行情况、 故障告警等各方面信息进行从全局到局部的可知和可控。

主要包括对应用的管理、 虚拟机的管理、 物理机的管理、 存储的管理、 网络的管理、 安全的管理以及机房的管理。

资源监管可对各类资源进行关联管理和从多视角进行逐级管理。

资源的监管是需要对应的厂商提供相应的信息和接口， 同时也需要一定量的二次开发， 因此以下功能的实现需分期逐步实现。

13.10.1.1 应用管理

应用的监控， 包括对物理资源运行的应用和虚拟机所运行应用的监控。

应用使用的资源： 监控应用所使用的基础信息， 根据云平台服务商提供接口的能力， 监控应用的 CPU、 内存等资源占用信息。

应用所在机器： 监控应用所在机器的主要性能， 如 CPU、 内存和磁盘性能。

应用健康状态的监控： 监控应用是否正常启动、 应用日志是否正常记录、 应用可否被正常访问等。

应用日志监控： 根据云服务商提供应用的监控的接口， 管理应用的日志并根据日志级别进行日志分级信息的监控， 根据安全审的条件发出不同级别的告警信息。

13.10.1.2 虚拟机管理

可对虚拟机按照不同的用户权限进行创建、 删除、 启动、 关闭、 重启、 修改、迁移等各类管理。

对虚拟机 CPU、 内存、 磁盘、 网络等资源的配置情况、 使用情况、 运行情况、所在物理机、健康状况、 故障监控、 运行时间、 关机时间等情况进行查看和管理。

可对虚拟机的生命周期进行管理， 如虚拟机的申请部门、 生存时间、 迁移情况、 应用情况等进行查看管理。

以上的管理系统都可以对变化的信息进行保存， 提供基于时间、 用户、 业务等单个或多个关键字的查询和统计， 并结合系统前台界面的请求， 对指定虚拟机的各种基本信息及动态信息结合图表方式进行展现。

13.10.1.3 物理机管理

可对物理机按照权限进行查看管理： 物理机所在机房、 机柜、 CPU 颗数和核数、 内存、 磁盘、 以及物理机所使用网络、 IP 地址等信息。

物理机的运行状况查看管理： CPU 使用率、 内存使用率、 磁盘 IO 性能及所用空间、 健康状况、 故障监控、 运行时间、 关机时间、 物理机内虚拟机等情况的管理。

以上的管理系统都可以对变化的信息进行保存， 提供基于时间、 用户、 业务等单个或多个关键字的查询和统计， 并结合系统前台界面的请求， 对指定物理机的各种基本信息及动态信息结合图表方式进行展现。

13.10.1.4 存储管理

根据用户权限的不同， 可对存储设备进行以下操作：

1 、 启动、 关闭、 重启、 修改等各类管理。

2、 卷/ 卷类型的创建、 升级、 删除、 查询等操作。

3、 快照的创建、 升级、 删除、 查询等操作。

4、 查看存储设备的配置情况： 所在机房、 机柜、 硬盘数量、 硬盘配置、 IO 等信息。

5、 查看存储设备的运行情况： I/O 性能、 存储空间使用情况、 卷、 快照、设备健康状况、故障情况、 运行时间、 关机时间等情况的管理。

以上的管理系统都可以对变化的信息进行保存， 提供基于时间、 用户、 业务等单个或多个关键字的查询和统计， 并结合系统前台界面的请求， 对指定存储设备的各种基本信息及动态信息结合图表方式进行展现。

13.10.1.5 网络管理

网络设备的配置情况： 所在机房、 机柜、 设备型号、 端口等信息。

网络设备的运行情况： CPU 内存利用率、 端口流量、 IP 分配、 健康状况、 故障监控、 运行时间、 关机时间等情况的管理。

以上的管理系统都可以对变化的信息进行保存， 提供基于时间的查询和统计， 并结合系统前台界面的请求， 对指定网络设备的各种基本信息及动态信息结合图表方式进行展现。

13.10.1.6 安全管理

通过与云服务商平台的接口， 收集各类安全设备的配置、 运行的信息以及系统中安全事件信息等进行收集、 查询、 展示和分析。

13.10.1.7 机房管理

通过与云服务商平台的接口， 查看机房相关信息， 包括机房温度、 湿度、 门禁、 监控视频等， 实现机房进行远程的监管。

13.10.1.8 硬件准入管理

对硬件准入的管理， 主要是对接入智慧园区大数据云平台云监管平台和云服务商平台的边界进行保护， 对接入网络的终端和终端的使用人进行合规性检查， 同时关联至云监管平台中。 只有被云监管平台激活的资源， 才能在云监管平台和云服务商平台上看到， 用于资源的申请和使用。 需要准入的硬件设备包括： 服务器、 存储、 网络、 安全设备及其他外围设备。

13.10.2 接口管理

云监管平台应具备与电子政务外网统一 CA 认证、 短信、 邮件等系统的接口。

13.10.3 运维管理

13.10.3.1 流程管理

智慧园区大数据云平台的管理涉及到不同政府部门的租户、 不同的云服务商、 各类监管部门等众多使用和管理角色， 因此对于系统的管理需要制定一些规范的制度和流程， 通过流程化审核和记录确保系统整体使用和运维的安全。

云监管平台的工单流程可以包括用户注册、 权限修改、 资源申请与释放、 故障申报与处理、工作协同、 硬件准入等， 可通过流程管理模块根据实际需求进行流程增减及流程修改， 实现可定制化。

13.10.3.2 监控告警管理

13.10.3.2.1 活动告警

活动告警是指系统被监控设备当前正在发生的告警信息。 系统管理员通过活动告警管理模块，及时地发现当前设备的告警信息， 及时地的解决设备的告警问题， 保证了设备的正常稳定的运行。

由于告警信息属于级别较低的警告信息， 系统管理员可以选择忽略和确认。

告警信息支持导出功能， 支持把系统中的告警导出生产文档。

13.10.3.2.2 历史告警

历史告警是指系统被监控设备以前发生的告警信息。 系统管理员通过历史告警管理模块， 可以查看设备过去的告警信息， 分析设备的负载趋势以及设备的健康状态， 对于管理员对设备运行情况的了解提供了重要信息和科学依据。

告警信息支持导出功能， 支持把系统中的告警导出生成文档。

13.10.3.2.3 活动故障

活动故障是指系统当前被监控设备正在发生的故障。 系统管理员通过活动故障管理模块， 及时地发现当前设备的故障信息， 及时地的解决设备的故障问题，保证了设备的健康稳定的运行。

由于故障信息属于级别高的警告信息， 颜色上会呈现红色， 在监控策略设置的前提下， 也会按照监控策略的规则进行触发相应的处理机制。

故障信息支持导出功能， 支持把系统中的故障导出生成文档。

13.10.3.2.4 历史故障

历史故障是指系统被监控设备以前发生的故障信息。 系统管理员通过历史故障管理模块， 可以查看设备过去的故障信息， 分析设备的存在的故障的原因， 对于管理员修复设备的故障提供了重要信息和科学依据。 故障信息支持导出功能，支持把系统中的故障导出生成文档。

13.10.3.3 系统消息提醒

在监管平台的使用过程中， 需要通过短信、 邮件等方式完成消息的下发， 如流程审批提醒、告警故障提醒、 资源状态提醒等， 需考具备短信、 邮件下发的功能性。 系统应具备单个用户发送、 按分组发送、 按角色发送等功能。

13.10.3.4 运维统计报表

以云监管平台中的各种信息为基础， 根据监管平台使用者的需求， 实时或周期性的生成各类报表， 以可视化图表的形式进行展示， 并可提供模板定制、 数据导出等功能。

依据对监测数据的自动汇聚、 抽取、 分析， 提供基础架构性能与告警、 资源比较、 指标排名、 指标趋势等各类层次化统计分析报表。 从业务运行状态到微观性能指标， 自定义查询业务应用系统及其关联资源的当前和历史运行情况。