自治区级政务云（专用业务）运维

服务采购工作方案

**2024年1月**

[一、项目背景 3](#_Toc6954)

[二、项目目标 3](#_Toc23735)

[三、运维内容和要求 3](#_Toc2550)

[3.1运维体系建立和优化 4](#_Toc10225)

[3.2基础设施运维 4](#_Toc10889)

[3.3云平台日常运维 5](#_Toc25624)

[3.3.1业务上云支持 5](#_Toc11932)

[3.3.2健康检查和处理 6](#_Toc30701)

[3.3.3资源监控和处理 6](#_Toc13840)

[3.3.4云平台优化与改进 7](#_Toc12113)

[3.4云平台安全运维 7](#_Toc25282)

[3.4.1租户安全运维 7](#_Toc31808)

[3.4.2设备系统安全 8](#_Toc8201)

[3.4.3网络安全演练 8](#_Toc214)

[3.4.4开展网络安全等级保护测评 9](#_Toc25380)

[3.4.5开展密码应用与安全性年度测评 9](#_Toc12936)

[3.5故障处理和应急处置 9](#_Toc5156)

[3.6重保运维服务 10](#_Toc10213)

[3.7应急演练 10](#_Toc2836)

[3.8灾备运维 10](#_Toc28062)

[3.9安全运营服务 11](#_Toc11116)

[3.10相关系统运营支撑服务 11](#_Toc25775)

[四、运维团队要求 12](#_Toc14354)

[五、运维软硬件清单 17](#_Toc31444)

[六、预算 23](#_Toc3194)

# 项目背景

2022年开展的自治区级政务云生产中心扩容及同城双活中心云资源建设项目建成的自治区级政务云（专用业务）主要提供厅局单位双活应用的部署。

主生产中心、同城双活中心的互联网区与公用网络区分别部署一套云平台，共计4个云平台，包括200多台服务器，100多台网络设备，60多台安全设备，以及杀毒软件、云平台管理软件、备份系统、虚拟化软件等系统软件。

# 项目目标

保障自治区级政务云（专用业务）的安全稳定运行，提高云平台的运行效率，消除信息系统瓶颈，能够更好地为政务系统提供基础平台服务，确保全区各机关单位建立的各类信息系统能够安全稳定运行。

# 运维内容和要求

本项目主要运维内容包括运维体系建立和优化、基础设施运维、云平台日常运维、云平台安全运维、故障处理和应急处置、重保运维服务、应急演练、灾备运维、安全运营服务、相关系统运营支撑服务等。

## 运维体系建立和优化

运维体系建立与优化。为实现自治区级政务云（专用业务）安全、运维策略的统一管理，提高云平台整体的安全、运维水平，建立一套符合信息系统等级保护三级的体系化管理目标和要求的安全运维管理制度与管理办法，如安全运维管理制度、云平台运维管理制度，进一步防范和控制系统故障和信息安全风险，保证云平台整体安全、可靠。

运维服务管理流程建立与优化。为加强和规范自治区级政务云（专用业务）运维管理工作，将运维工作标准化、流程化，制定运维服务管理流程并设计管理流程图与管理表单，内容包括但不限于：事件管理、问题管理、变更管理、人员管理、安全管理、基础设施运维管理、故障与应急管理等。

运维管理方案制定与优化。制定运维服务管理方案，结合项目实际情况不断深入优化、完善运维服务管理内容与范围，内容包括但不限于：工单等流程响应、日常例行工作、资源资产维护等。

制定故障管理方案、制定应急管理方案、制定云平台高可用演练与管理方案、制定备份与恢复管理方案。

## 基础设施运维

本项目设备资产主要包括服务器、存储、网络及安全设备等。对设备配置、安装位置、IP地址、用途、厂商等信息进行统一登记，建立和维护设备台账表，及时更新台账记录，定期盘点，保证账实相符。管理设备出库、入库，按照相关规定办理设备出、入库手续，形成设备出入库文档。

本项目运维的设备资产包括200多台服务器，100多台网络设备，60多台安全设备，以及杀毒软件、云平台管理软件、备份系统、虚拟化软件等系统软件。设备清单详见《运维软硬件清单》。

## 云平台日常运维

自治区级政务云（专用业务）面向全区14个设区市和200多家区直单位提供云资源服务，目前已分配30多家单位100多套系统，虚拟机总数约3000台，每套系统和虚拟机均涉及云平台日常运维工作。如云平台健康检查（巡检）及日常维护、云平台日常问题处理、云平台资源使用情况和使用趋势分析、云平台网络、安全和运行优化等。

### 业务上云支持

承担云平台业务上云的资源评估和技术交流，根据业务实际需要提出资源需求规划建议。接收、规划并资源需求，包括计算、存储、网络、安全、备份等云平台资源，以及堡垒机、云租户管理员、VPN等账号或权限资源。

响应管理单位安排的对云平台资源、托管资源的服务需求，提供技术咨询和资源分配服务，并指导和协助业务应用部署、调试、使用和管理相关资源。包括计算资源池、网络资源池服务、存储资源池、安全资源池等。

云平台操作系统模板安全加固，定期对已分配资源的服务器和应用服务进行漏洞扫描和安全检查，指导和协助业务系统进行安全加固、漏洞修复、安全资源池配置。

### 健康检查和处理

为了保障业务和系统的稳定运行，运维人员需要对云平台的资源、告警、性能、容量、应用等使用情况进行全方面集中监控，及时了解运行状况，识别风险隐患，减少和预防事故的发生。当发生异常时及时通知相关人员，避免问题发酵扩大影响范围。

使用工具或手动方式，定期对平台进行巡检，生成巡检报告，并根据报告发现问题进行配件更换、补丁升级等操作，减少系统隐患，确保云平台能够长期安全、稳定、可靠地运行，降低维护成本。

涉及云平台管理平面、网络平面、业务平面和存储平面的健康检查和问题处理。

### 资源监控和处理

监控物理资源、资源池、云资源、云服务系统的性能、资源状态等，全方位监控云数据中心的整体状况。每天定期监控物理设备、资源池和云服务的整体告警信息，保障系统的正常运行。

### 云平台运行分析

针对云平台IaaS资源池、租户VDC资源分析，根据历史数据报表信息，了解并分析设备数量、资源利用率、容量统计、告警趋势等的分布、趋势。对于频发告警的部件或节点要进行分析、优化，提高系统稳定性。

按周、月、季、年输出资源使用情况报告。

### 云平台优化与改进

通过日常运维工作或定期高可用演练，及时发现云平台存在的安全运行隐患，如云平台、服务器、安全、网络、存储等设备存在的配置不合理问题或产品潜在BUG等，及时提出相关优化改进建议，推进产品供应商解决配置问题或产品BUG，组织相关产品供应商执行优化调整动作，不断优化云平台整体性能，不断提高云平台高可用、高可靠能力。

## 云平台安全运维

自治区级政务云（专用业务）面向全区14个设区市和200多家区直单位提供云资源服务，目前已分配30多家单位100多套系统，虚拟机总数约3000台，每套系统和虚拟机均涉及云平台安全运维工作。

### 租户安全运维

根据云平台租户申请及业务需求，提供安全方案并协助开通安全资源池策略。

每月对云平台租户虚拟云主机进行漏洞扫描，输出漏洞扫描报告，并通过邮件方式发送租户；每月对云平台宿主机、网络设备、安全设备等进行漏洞扫描，输出漏洞扫描报告并修复。

对网络中存在的风险行为进行实施监控（通过态势感知、防火墙、IPS等安全设备/系统），对监控中发现的风险行为配合安全厂商进行风险评估；根据风险评估情况协调租户、安全厂商商定并输出风险处理方案，并对风险进行控制措施。

通过安全态势感知平台，对网络中发生的安全事件进行监控，识别高风险行为并及时上报，制订通报机制，通报云租户进行安全整改，通过安全设备或系统及时开展防御措施防止高风险事件进一步发展。

### 设备系统安全

云平台安全设备巡检、配置、升级、维护。

所有运维终端安装计算机防病毒软件，对防病毒软件系统进行监控，并记录病毒查杀情况。

定期更新云平台各区安全设备特征库，确保特征库为最新特征库，保障内部网络安全。

及时跟进各产品的安全漏洞信息和产品厂商发布的安全补丁信息。

及时通知云平台租户操作系统补丁，指导和协助租户开展补丁修复工作。

### 网络安全演练

组织开展的网络安全实战演习的防守任务，提供网络安全实战演习防守方案、攻击监测、调查取证、事件抑制、事件根除和分析总结，提交《安全实战演习防守报告》。

### 开展网络安全等级保护测评

依据《网络安全等级保护基本要求（GB∕T 22239-2019）》及《网络安全等级保护2.0指导规范》，每年开展云平台的网络安全等级测评。并配合单位协助开展业务系统的网络安全等级测评。

### 开展密码应用与安全性年度测评

依据《GB/T39786-2021 信息安全技术 信息系统密码应用基本要求》及信息系统等级保护要求，每年开展云平台的密码应用与安全性测评。

## 故障处理和应急处置

当业务系统、云平台出现故障或突发事件，导致服务质量下降或服务停止时，运维人应根据故障管理要求及时完成故障排查、应急恢复、问题定位、故障处理、输出故障报告等工作。

根据自治区级政务云（专用业务）故障处理流程和应急预案，制定故障定级、升级和处理要求，确保能够指导解决云平台突发故障。

根据风险评估情况，对有可能造成损失的系统，优先制定应急方案，并在发生问题时优先启动、优先恢复。

定期组织有关人员分析研究应急管理工作中出现或可能出现的新情况、新问题，及时更新应急方案，保证应急措施的切实有效，能够达到实际目的和预期应用效果。

## 重保运维服务

重要保障时期（国家和自治区各种重大活动、会议、节假日等）对可能出现影响业务稳定性的安全风险进行重保前的安全漏洞扫描和检测、安全监测、安全分析、事件应急等工作，完成重保后的重保总结报告输出。

|  |  |  |  |
| --- | --- | --- | --- |
| 节假日、重要会议、重要活动时间表 | | | |
| 序号 | 重要保障名称 | 时间 | 天数  （预估） |
| 1 | 元旦期间的安全重要保障 | 依当年假期制定 | 1 |
| 2 | 春节期间的安全重要保障 | 依当年假期制定 | 8 |
| 3 | 全国两会期间的安全重要保障 | 时间待定 | 10 |
| 4 | 清明期间的安全重要保障 | 依当年假期制定 | 3 |
| 5 | 三月三期间安全重要保障 | 依当年假期制定 | 3 |
| 6 | 五一期间的安全重要保障 | 依当年假期制定 | 5 |
| 7 | 端午期间的安全重要保障 | 依当年假期制定 | 3 |
| 8 | 护网期间的安全重要保障 | 时间待定 | 7 |
| 9 | 东盟期间的安全重要保障 | 依当年假期制定 | 5 |
| 10 | 中秋期间的安全重要保障 | 依当年假期制定 | 3 |
| 11 | 国庆期间的安全重要保障 | 依当年假期制定 | 7 |
|  |  | 合计 | 55 |

## 应急演练

编制云平台相关产品，包括基础设施、网络系统、安全系统、云平台侧的高可用演练、应急演练和故障处理演练方案。组织各相关方定期进行高可用演练、应急演练和故障处理演练工作。并配合租户开展自身应用系统的应急演练工作。

## 灾备运维

本项目包含一个生产中心和一个异地备份中心，其中生产中心和同城双活中心使用备份容量约2PB，异地灾备中心复用贵港异地灾备中心存储容量，实现数据级备份。

承担各用户单位备份需求的资源评估和技术交流，响应各用户单位的需求工单，并根据用户单位实际数据备份需要提出备份任务规划建议，实现政务云系统的数据备份。

定期开展灾备数据有效性验证、制定备份与恢复管理方案、执行灾备演练。

## 安全运营服务

制订完善的应急响应处理预案和日常维护作业计划，并坚决落地执行，按计划完成日常巡检、应急演练、漏洞扫描及渗透测试等工作，确保政务云平台能够更加稳定运行。

面向云租户的安全服务体系应全面覆盖事前、事中、事后3个阶段：事前阶段采取安全扫描、情报预警、评估加固及培训演练等措施，防止发生安全事故；事中阶段采取安全监测分析、安全防护、安全接入及网站防护等措施，以抵御黑客攻击；事后阶段在处置过程中，可根据安全事件严重程度进行安全事件处置或应急响应，确保安全事件发生后能够快速处置。

## 相关系统运营支撑服务

安全态势感知运营支撑。通过安全态势感知系统进行合规及符合性检查、资产发现与体系化运营、脆弱性监测与防护分析、威胁分析与响应处理、防御策略优化、威胁情报分析等运营工作。

数字应用安全监测平台支撑。包括开源软件威胁情报治理，攻击及防御策略优化及处置，漏洞人工核验和处置分析验证，运行时免疫防护运营，按月输出分析月报及整改情况报告，并按季度按年度输出对应的数据应用安全监测报告。

防病毒支撑服务。提供自治区政务云（专用业务）租户虚拟机防病毒防护，定期更新控制中心病毒库，进行控制中心全局策略配置。

VPN系统支撑服务。负责进行VPN系统设备运维，以及账号开通、权限设置、密码设置、登录异常处理、VPN故障处理等工作。

产品供应商管理。负责对云平台所涉及的产品或服务供应商进行管理，包括人员监管、配置核查监管、方案文档审核、操作设置监管、备品备件监管、培训管理、产品升级管理等。

维护文档管理。管理和收集本项目的日常运维工作中所产生的过程文档，包括电子类文档和纸质类文档，例如：运维日报、项目相关报告及材料、维护工单、系统升级文件、机房巡检单等。针对日常运维、定期巡检等主要工作内容编制维护手册，建立完备的维护过程文档资料，统一格式、做好分类，根据信息技术和信息安全的发展趋势和运维工作的实际情况定期更新手册内容，最终建成维护文档库。

# 运维团队要求

在服务期内，要求提供不少于15人的驻场运维团队，人员要求至少大学本科以上学历，且团队具备中级职称以上人员占比不少于40%。

运维人员队伍参照ITIL/ITSS标准建立，其中一线运维人员满足日常维护和值班保障要求不少于7人，任职要求大学本科以上学历，至少1年以上相关工作经验；二线运维人员按专业岗位设置，包括原厂运维工程师，每个专业岗位至少1人，任职要求大学本科以上学历，至少3年以上相关工作经验，具备丰富项目经验且条件优秀者可适当放宽学历限制。

运维岗位至少包括运维经理岗、综合运维岗、设备运维岗、资产管理岗、网络运维岗、安全运维岗、云平台运维岗、系统运维岗、原厂运维岗等，具体内容如下：

其中，综合运维岗、业务支撑岗、设备运维岗、安全运维岗、云平台运维岗，共10人实行轮岗及7\*24小时值班制（白班4人，中班2人，夜班2人，夜班人员第二天轮休。固定值班人员共10人。）值班期间同时负责上述岗位各项工作；其次重保及其他单位要求的特殊时期安全运维岗及网络运维岗参与值班。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **岗位名称** | **岗位等级** | **主要职责** | **岗位定员** | **岗位要求** | **备注** |
| 1 | 运维经理 | 二线 | 主持整体运维工作，重大事项及故障对接、解决，对单位做好各项沟通工作，协调对接后台等各个资源，把握技术方案，应急响应处置等工作。 | 1 | 1)研究生及以上学历，掌握服务规划、设计、管理等方面的专业知识; |  |
| 2)具备专业任职资格证书,具备国家计算机和软件资格考试中级以上资格或IT服务项目经理资格; |
| 3)具有5年及以上大型网络、虚拟化、云计算实施管理经验。 |
| 2 | 综合运维岗（含档案管理） | 一线 | 1、运维工单接收  2、突发事件处理：定期检查系统运行状态，确保各项服务正常运作。3、考勤管理：负责运维团队人员考勤工作，发布每日值班及轮休人员名单。4、信息统计及报表编制5、运维档案管理6、回访及满意度调查。 | 2 | 1)专科以上学历； | 7\*24小时值班制 |
| 具备国家计算机和软件资格考试中级及以上，或具备主流网络厂商中级及以上资格认证; |
| 3)具有1年及以上中小型网络、虚拟化、云计算交付和运维经验。 |
| 3 | 业务支撑岗 | 一线 | 1、7\*24小时对业务系统的日常监控与维护。2、处理云平台用户的资源申请和安全需求。3、监控及整理云平台资源情况。4、业务系统故障处理及支撑。 | 3 | 1)本科以上学历，具备计算机网络专业知识； 2) 具备国家计算机和软件资格考试中级及以上，或具备主流网络或网络安全厂商、操作系统厂商中级及以上资格认证; 3)具有3年及以上中小型网络、虚拟化、云计算交付和运维经验。 | 7\*24小时值班制 |
| 4 | 设备运维岗 | 一线 | 1、负责云平台多个机房相关设备的日常巡检和维护，设备维护操作管理，编制整理设备巡检记录。  2、对接设备厂商、其他运维岗完成设备故障处理，编制整理硬件故障处理记录。  3、备品备件管理， | 2 | 1)专科以上学历，具备计算机网络专业知识； | 7\*24小时值班制 |
| 2)具备国家计算机和软件资格考试中级及以上，或具备主流网络厂商初级及以上资格认证; |
| 3)具有1年及以上项目管理或弱电工程实施经验。 |
| 6 | 网络运维岗 | 二线 | 负责网络设备的配置维护，监控网络设备状态、性能、连通性等运行状态，进行流量或性能趋势分析，不断进行网络配置的优化评估和执行工作，监控平台网络告警配置，及时处理网络中断、网络设备故障等。 | 1 | 1)本科以上学历，具备计算机网络相关专业知识； |  |
| 2)具备国家计算机和软件资格考试中级及以上，或具备主流网络厂商中级及以上资格认证; |
| 3)具有3年及以上中大型网络规划、实施、运维经验。 |
| 7 | 安全运维岗 | 一线 | 1、负责安全设备的配置维护，规划、执行和记录安全配置策略，监控安全系统及网络安全运行状况，安全事件应急处理、分析总结并提出优化方案，执行安全计划工作，编制安全工作报告。 | 2 | 1)本科以上学历，具备计算机网络、信息安全、云计算相关专业知识； | 7\*24小时值班制 |
| 2)具备国家计算机和软件资格考试中级及以上，或具备主流网络、信息安全及虚拟化厂商中级及以上资格认证; |
| 3)具有3年及以上运维经验并具备二/三级等保实施交付经验。 |
| 8 | 云平台运维岗 | 二线 | 1、云平台日常维护，补丁及升级管理。2、云平台深度巡检与优化。3、云平台和网络安全设备配置审计，值班人员负责云平台及网络设备操作动作和命令复核。4、攻防演练的技术支持。 | 1 | 1)本科以上学历，具备计算机网络、信息安全、云计算相关专业知识； | 与原厂驻点7\*24小时值班制 |
| 2)具备国家计算机和软件资格考试中级及以上，或具备主流网络、信息安全及虚拟化厂商中级及以上资格认证; |
| 3)具有3年及以上存储、超融合、虚拟化、容器实施交付和运行维护管理经验。 |
| 9 | 二线 | 1 | 华为云原厂运维 | 华为原厂工程师报价 |
| 10 | 系统运维岗 | 二线 | 1、业务系统资源使用情况评估，存在冗余资源及时上报。  2、业务系统部署上线技术支持。  3、业务或管理系统账号分配及权限管理，如增加、删除用户、重置用户密码、管理用户权限等。 | 1 | 1)本科以上学历，具备计算机网络、信息安全、云计算相关专业知识； |  |
| 2)具备国家计算机和软件资格考试中级及以上，或具备主流网络、操作系统、软件开发厂商中级及以上资格认证; |
| 3)具有3年及以上政务业务系统运行维护管理经验。 |
| 11 | 数据安全岗 | 二线 | 1、数字应用安全检测系统运维、日常监测、输出监测报告。 | 1 | 1)本科以上学历，具备计算机网络、信息安全、渗透测试与安全攻防等相关专业知识； |  |
| 2)具备国家信息安全水平考试一级及以上，或具备CNVD原创漏洞证明资质证书; |
| 3)具有2年及以上网络安全产品的实施与运维，渗透测试，攻防演练以及平台防护管理经验。 |
| **人数合计** | | | | **15** |  |  |

# 预算

每年预算200万元，服务期三年，总体预算600万元。详见下表。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **单位：万元** | | | | | | |
| **序号** | **项目名称** | **单位** | **数量** | **单价** | **小计** | **备注** |
| 1 | 运维经理 | 人/年 | 1 | 15 | 15 |  |
| 2 | 综合运维岗（含档案管理） | 人/年 | 2 | 10 | 10 |  |
| 3 | 业务支撑岗 | 人/年 | 3 | 11 | 11 |
| 4 | 设备运维岗 | 人/年 | 2 | 10 | 10 |
| 5 | 网络运维岗 | 人/年 | 1 | 11 | 11 |  |
| 6 | 安全运维岗 | 人/年 | 2 | 11 | 11 |  |
| 7 | 云平台运维岗 | 人/年 | 1 | 11 | 11 |
| 8 | 华为原厂驻点 | 人/年 | 1 | 24 | 22 |  |
| 9 | 系统运维岗 | 人/年 | 1 | 11 | 11 |  |
| 10 | 数据安全岗 | 人/年 | 1 | 10 | 12 |  |
| 11 | 重保服务 | 天 | 55 | 0.27 | 0.27 |  |
| 12 | 网络安全攻防演练 | 人/天 | 63 | 0.12 | 0.12 |  |
| 13 | 网络安全检查/评估 | 人/天 | 5 | 0.12 | 0.12 |  |
| 总价 | | |  |  | 200.1 |  |