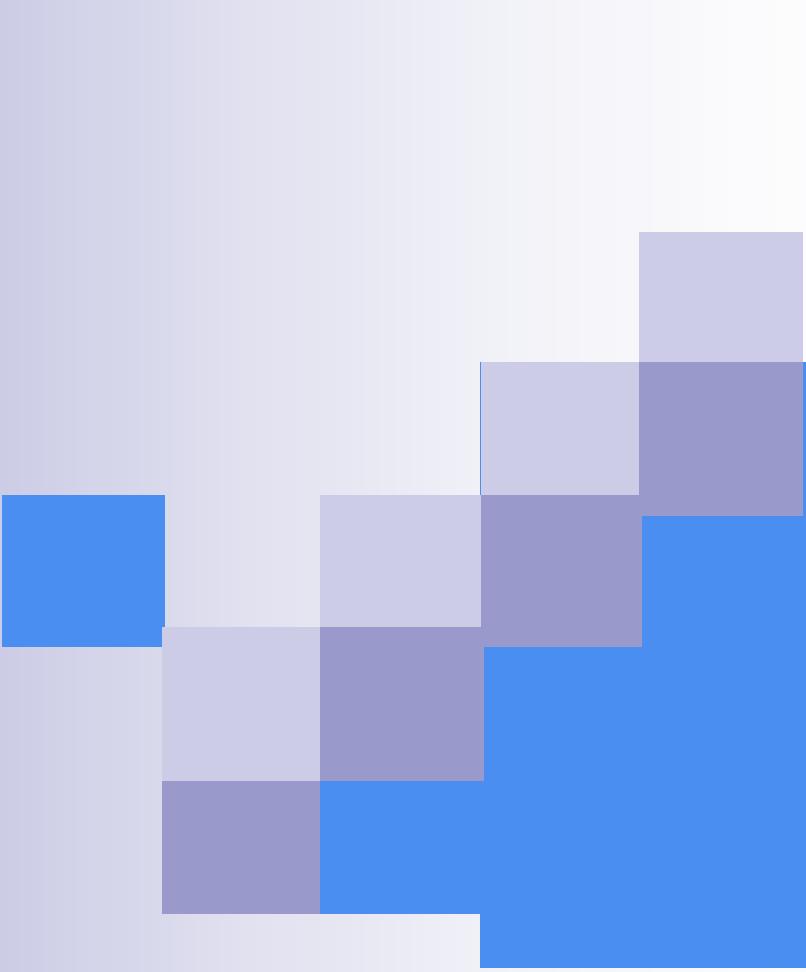




国泰新点软件股份有限公司

项目部署准备

基础设施支持部

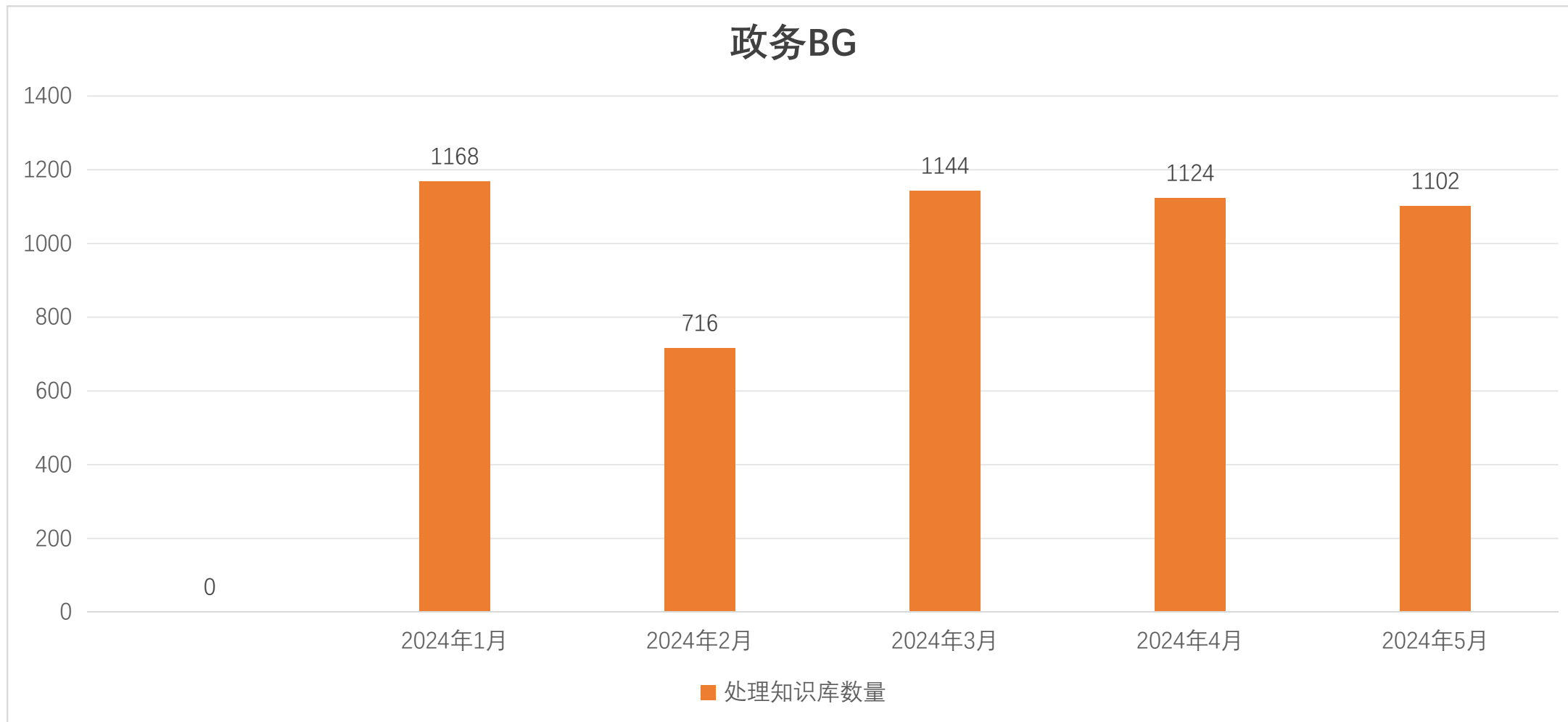
2024-06

目 录

- 1、 部署人员现状
- 2、 部署流程说明
- 3、 做部署准备
- 4、 FAQ

部署人员现状

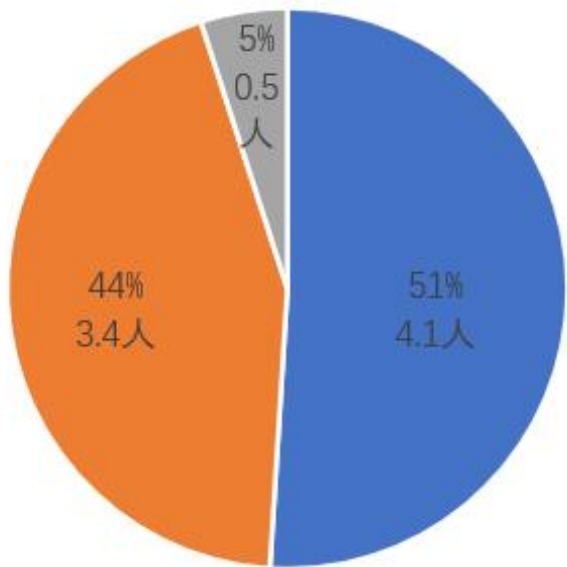
基础设施支持部现有部署人员合计15人，除系统部署之外，还需处理大量知识库。
下图为基础设施支持部 仅政务BG 2024年的知识库处理数量



部署人员现状

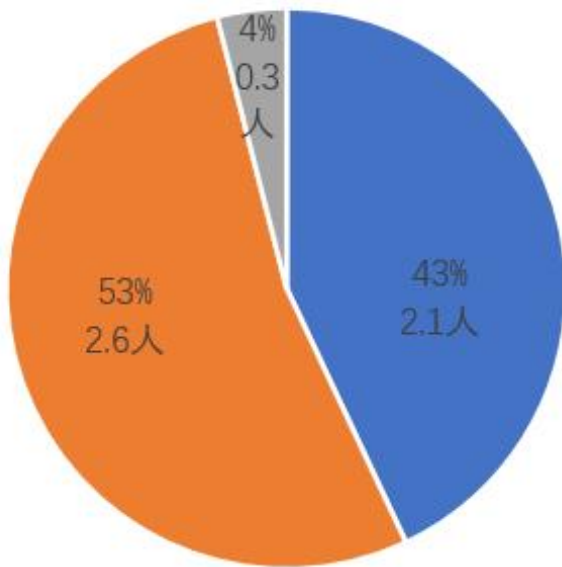
基础设施支持部现有部署人员的工作投入占比，部署只占日常中的**50%**。

政务BG
工作量占比和人力



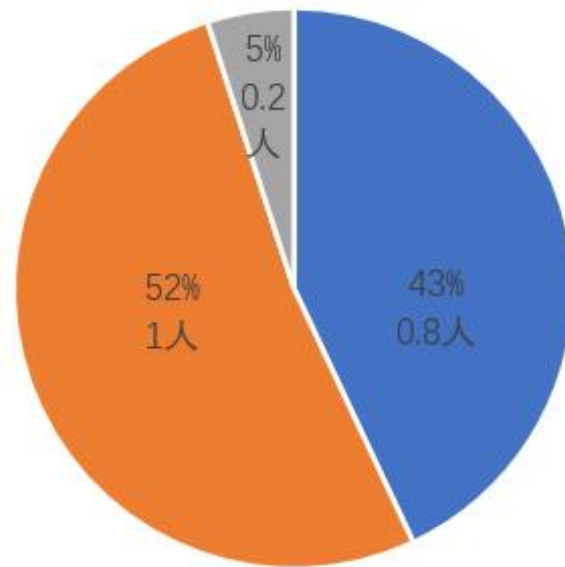
■ 知识库 ■ 项目部署 ■ 系统迁移

交易BG
工作量占比和人力



■ 知识库 ■ 项目部署 ■ 系统迁移

建设BG
工作量占比和人力



■ 知识库 ■ 项目部署 ■ 系统迁移

部署人员现状

基础支撑部署资源池有限

部署资源池不仅仅支撑项目部署

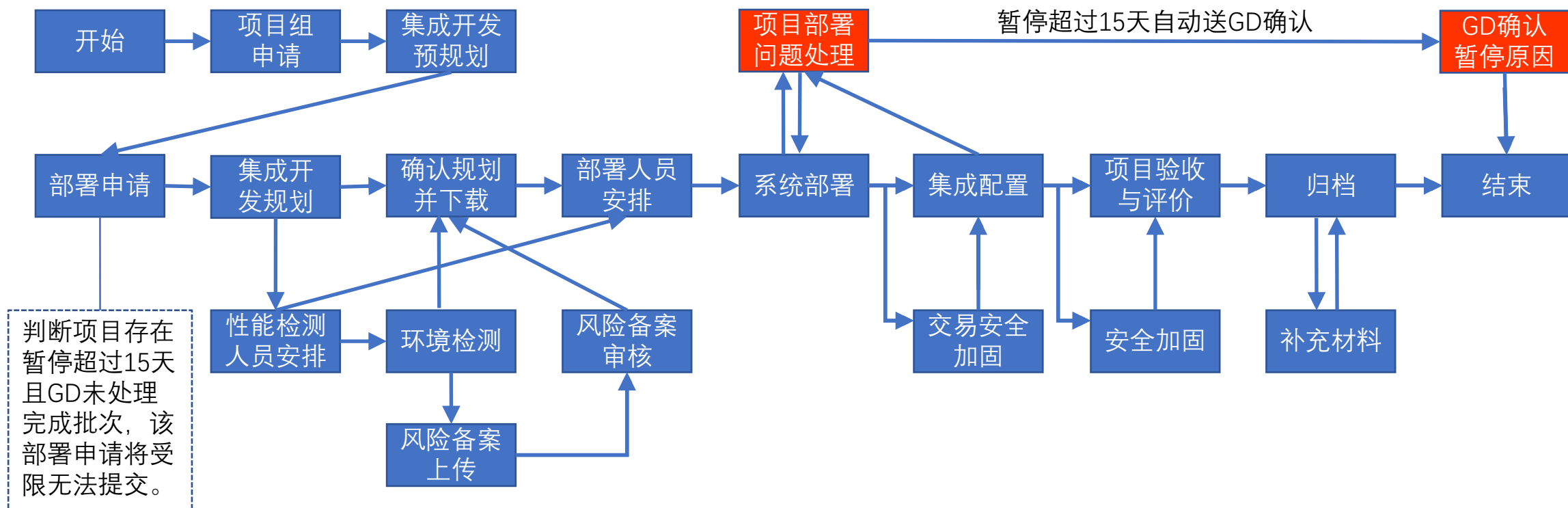
项目部署不是仅依赖基础支撑部署人员就可以快速完成的。

需要部署流程各环节尽责做好各自的负责工作，才能快速完成项目部署工作

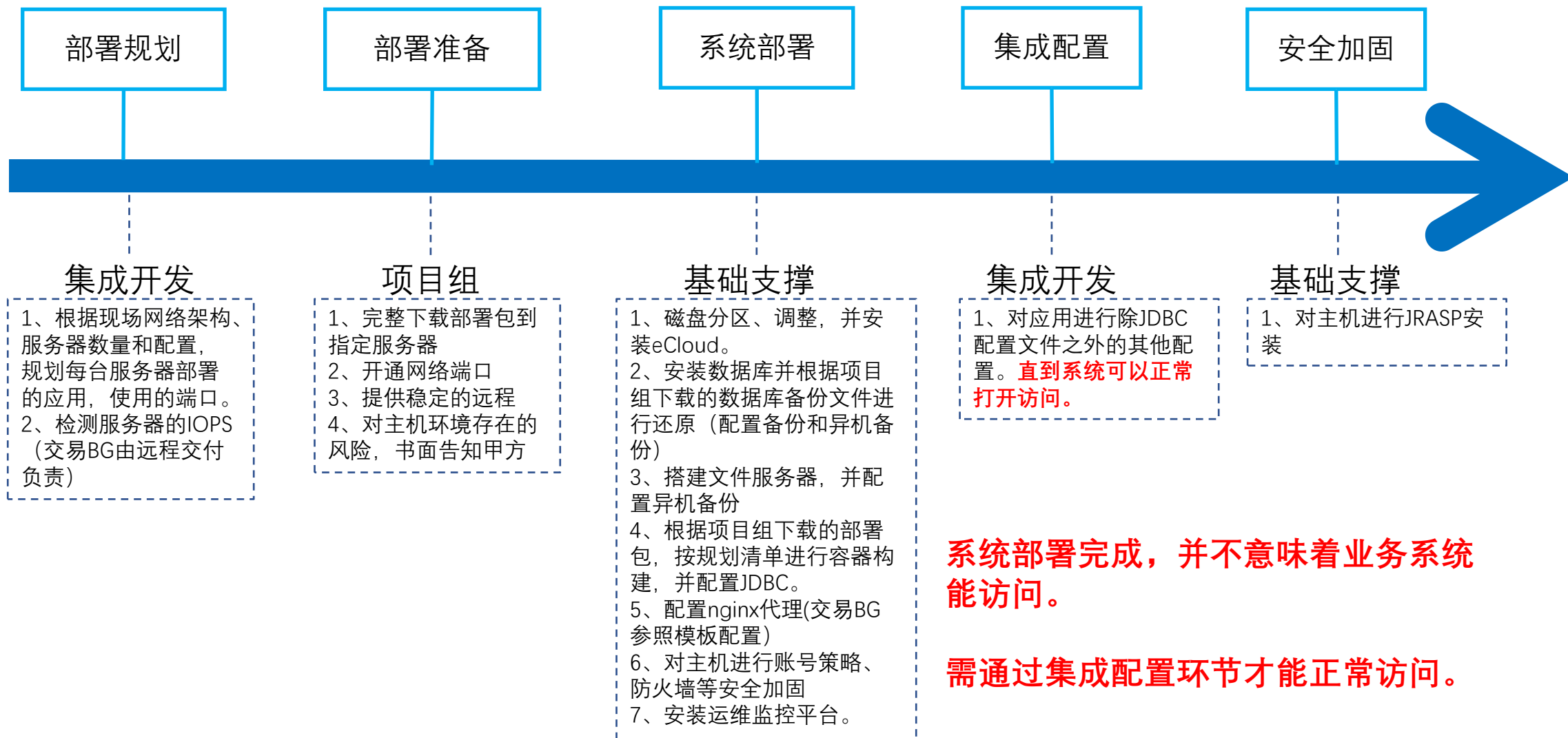
目 录

- 1、 部署人员现状
- 2、 部署流程说明
- 3、 做部署准备
- 4、 FAQ

部署流程说明



部署流程说明-主要环节





目 录

- 1、 部署人员现状
- 2、 部署流程说明
- 3、 部署准备
- 4、 FAQ

部署准备-部署申请填写信息

部署要求

部署性质:

部署内容: ☒ 应用服务/组件 ☐ 数据库

远程/现场部署: ☒ 远程部署 ☐ 现场部署

有无异机备份服务器: * ☒ 有 ☐ 没有

是否eCloud部署: ☐ 否 ☒ 是

是否国产化: * ☐ 是 ☒ 否

时间同步方式:

是否接入堡垒机: ☒ 是 ☐ 否

CPU类型: *

其他要求

是否网络隔离: ☐ 是 ☒ 否

使用HTTPS: ☐ 是 ☒ 否

是否部署运维监控平台: ☒ 是 ☐ 否

运维监控平台类型: * ☒ 网络版 ☐ 单机版 备注: 纯内网环境适用单机版, 与远程交付确认, 选择网络版, 则report IP 必填, 只能为IP类型。

期望排队周期: 天 备注: 2天及之内的, 且该条线对应的部署人员都存在部署工作, 自动发插队邮件

运维监控平台信息查看: [信息查看](#)

运维监控report IP: 备注: 运维监控平台上报服务器 (report) IP 地址, 非eCloud的IP, 除非report部署在了eCloud服务器上。

部署服务器数量: 台

部署应用数量: 个 备注: 2台服务器上部署同一个应用, 则部署该应用数量为2

补充信息

跳板机地址: *

部署包存放跳板机目录: *

信息如实填写准确

部署准备-常见问题

按遇到的问题数量从高到低，主要有以下部署准备问题。

- 1、部署包下载不完整
- 2、网络端口不通
- 3、服务器规划存在问题
- 4、涉及增量部署、迁移部署，历史信息反馈不准确
- 5、现场忙，没有时间配合部署。
- 6、服务器账号密码不正确，无法远程

部署准备-部署包

使用新点易维下载完整部署包，注意检查数据库备份文件有无下载。

★ 首页 🔥 App 和扩展 📁 部署包下载器 x							
< 返回 开始作业 > 1 录入部署编号 2 部署包内容确认 3 投递下载任务							
产品线	产品名称	版本	制品名称	制品种类	主机 IP	MD5	操作
	Windows_ywjreport	Windows_X64	Windows_ywjreport.zip	部署包		6ecbf1b1647a83caba09e7bc3309cff	重新下载
中央研究院	RegistryTools	X86	RegistryTools_INSTALL_x86_64_2024-03-26_22-04-17.bin	部署包		7c7f1cdb3c1fad9c6588db3f9ac1dd28	重新下载
中央研究院	eCloud_Agent	V3.0	eCloud_Agent_INSTALL_2024-04-25_17-02-18_3.bin	部署包		84e2c5b2dc0b7fa2a3c72c6a9439f70a	重新下载
中央研究院	eCloud_Server	V3.0	eCloud_Server_3in1_INSTALL_3_2_2024-04-29_13-56-22_3.bin	部署包		a828c37fa98b4f22c52c54544eb0e2d8	重新下载
	Windows_ywjcollect	Windows_X64	Windows_ywjcollect.zip	部署包		b8df7c026abccd66c97e56bfab3ea7b0	重新下载
	Linux_ywjreport	Linux_X64	Linux_ywjreport.bin	部署包		f29d2818ce648c74f53538885c75b787	重新下载
	sysbench	X86	sysbench_bin_aarch64_2023-04-14_00-05-51.bin	部署包		45f92851f47e0a021ff6c689a16245ec	重新下载
	Linux_ywjcollect	Linux_X64	Linux_ywjcollect.bin	部署包		be03fe4e1700d50b09654f4889523584	重新下载

部署准备-端口开通

一旦端口未开通好，可能直接导致部署暂停，或部署后应用无法访问。

如某项目增加了SOA节点从1台增加到4台，压测时新增的3台SOA没有压力。排查发现nginx与新增的3台SOA服务器之间端口不通。

如何避免：

- 1、项目组应了解项目网络情况，确认服务器所处网段，同网段服务器之间是否也存在隔离情况。并将网络情况反馈给集成开发，以便集成开发规划，并提供需要开通的端口地址给项目组。
- 2、根据集成开发提供的端口地址，找甲方对应部门/人员申请开通端口。
- 3、使用基础设施支持部提供的工具进行端口检测，确认端口开通好。

https://fdoc.epoint.com.cn:3366/epoint_deploy_book/Product_deploy/Know/envprepare/probeport.html

部署准备-部署包

个性化部署包，无法通过新点易维下载，需要联系开发提供完整。

部署包应包含应用程序和数据库备份文件两部分。

- 开发提供部署包时，需要提供对应的应用程序与数据库备份文件的对应关系，以及还原的数据库名称。
- 如数据库名称与数据库服务器上已有的名称重复。需给出处理意见（覆盖OR换数据库名称）。

部署准备-规划问题

部署人员按集成开发规划的清单和应用进行部署时，项目组要求调整应用所在服务器，将导致流程被暂停（集成开发与项目组进行拉通）或流程被退回。

如何避免：

- 1、部署流程提交时，服务器清单填写正确。否则正式开始部署时，部署人员发现服务器IP与规划不一致，将导致无法部署。
- 2、部署流程有一个环节“确认规划并下载”，该环节需项目组确认规划有无问题，并下载部署包。从而避免部署人员开始部署时，项目组提出需要调整服务器，进而导致部署流程被退回重新排队，增加了排队时长。

部署准备-项目历史信息反馈不正确

增量部署、迁移部署涉及项目历史信息不正确，如eCloud平台的密码不正确，项目使用新数据库服务器还是历史数据库服务器等。

如何避免：

1、项目组应有一份台账资料，知道项目有多少台服务器，每台服务器部署了哪些，相关平台的账号密码，该资料提供配合基础支撑部署的项目组人员。便于给规划人员参考，给部署人员和集成配置人员答疑。

部署准备-项目组忙无法部署

流程到系统部署环节，部署人员联系项目组进行部署时，项目组配合人员反馈忙。

如何避免：

- 1、项目组提前安排好配合部署的人员，避免开始部署时找不到项目组人员，导致流程被暂停。

部署准备-服务器无法远程

部署人员开始部署时，发现VPN连不上、服务器登录密码不正确等情况。

如何避免：

- 1、项目组提前确认好VPN，避免多人争抢VPN。
- 2、提前登录服务器，验证部署涉及服务器的密码正确，服务器均能登录上。
- 3、能通过新点易维连接的服务器，尽量通过新点易维维护好服务器信息。便于快速登录和批量执行脚本，提高部署效率。



部署准备-其他问题

磁盘性能太低，导致部署速度非常慢，且部署后往往会被铲掉重新部署。

需要部署集群，但没有提供虚拟IP地址。

没有跳板机（如windows或带图形界面的Linux），导致部署时无法验证。

如何避免：

- 1、测试IOPS，建议给出性能风险告知同时，补充部署成本增加风险。多一次部署，就是增加一次成本。
- 2、了解虚拟IP，如使用集群，需提前准备好虚拟IP（项目如使用数据库集群、nginx集群等，在规划环节与集成开发沟通确认是否需要虚拟IP）。

https://fdoc.epoint.com.cn:3366/epoint_deploy_book/Product_deploy/Know/envprepare/MySQL%20MHA%E6%90%AD%E5%BB%BA%E7%8E%AF%E5%A2%83%E5%87%86%E5%A4%87.html

- 3、规划环节与集成开发沟通，需规划一台跳板机（windows或带图形界面的Linux）。



目 录

1、 适用范围

2、 流程介绍

3、 部署申请

4、 FAQ

如何快速填写增量部署申请

成开发平台

陕西省公共资源交易平台

97

樊斌 副经理
基础设施支持部

系统管理

部署申请

部署申请

刷新

申请

复用并新增

关联预规划并新增

删除

部署架构图

老部署管理系统入口 (仅供查询)

高级搜索 >>

Q 请输入部署编号

☐	进程	序	部署编号	项目名称	申请人	申请日期	总耗时...
☒	▼	1	BSGL20231123004	陕西省公共资源交易平台	武琦琦(新...	2023-11-23 09:27	19.00天
部署申请 0天0时34分 集成开发规划 1天8时27分 性能检测人员安排 2天15时10分 环境检测 0天9时0分 风险备案上传 1天8时9分 风险备案审核 0天14时41分 确认规划并下载部署包 0天0时27分 部署人员安排 0天16时44分 系统部署 5天23时21分							
☐	>	2	BSGL20231110024	陕西省公共资源交易平台	张松(新点...	2023-11-14 14:39	217.08天
☐	>	3	BSGL20231025010	陕西省公共资源交易平台	武琦琦(新...	2023-10-25 11:32	8.94天
☐	>	4	BSGL20231024059	陕西省公共资源交易平台	张松(新点...	2023-10-24 16:59	26.89天

关于部署插队

基础支撑侧无法评估是否紧急需要插队，通常一天会遇到多个项目提出需要插队。

部分项目组申请插队，最终经过相关领导协调同意插队后，部署过程中发现部署准备工作未做好，部署超过要求完成时间要求一周。

- 做好进度规划，提前规划好部署时间，并做好部署准备，同时避免前置环节拖沓导致部署时间被压缩（如明确三方资源提供的最迟期限，当超过期限，则对应上线演示时间也顺延。）
- 部署插队需项目组发邮件给条线交付侧领导，部署人员安排后，可以提供部署人员正在部署、排队部署的顺序，由条线交付领导协调确定插队顺序。（2024年正在逐步取消部署人员的条线限制以提高部署人员的工作均衡度，将导致条线交付领导不仅仅协调自己条线内的项目，还需协调其他条线项目）
- 确实紧急的部署，部署准备工作扎实，避免因部署准备不好被暂停部署。

关于部署排队

由于部署人员有限（平均每个分公司只能分配到0.5个部署人员），且部署人员还需要被抽调单独支撑某些项目，目前只能通过部署排队来进行部署工作安排。

部署排队顺序为：部署人员正在部署批次、排队批次、暂停批次的时间顺序。

例如 部署人员6月18正在部署批次为 A B ， 暂停批次 C D ， 排队批次 E F，当天完成A批次部署，则6月19日无新增部署批次情况下，排队顺序为 B-E-F-C-D。

当6月19日上午 8：30收到新增部署批次 H，D批次暂停问题解决好，9：00将流程重新返回给部署人员，则排队顺序为 B-E-F-H-D-C。（暂停批次将重新进行排队，不具备优先部署权）

关于部署暂停处理

项目组原因导致部署暂停，流程将自动提交给项目进行部署暂停问题处理。

项目组收到部署暂停待办后，有两个按钮需注意：

- 1、部署暂停并终止流程，将导致流程送GD确认后结束部署（不可逆）。
 - 2、暂停问题处理完成，则将流程送回发起暂停人员继续部署或集成配置
- 其中部署暂停并终止流程按钮名称近期将调整为中止部署流程，避免误操作。

部署人员部署完系统，项目没有部署完成

部署人员部署完系统，只是系统部署到服务器上，还不具备使用条件，需经过集成配置、安全加固，直到通过项目组验收才算部署完成。

项目部署后，没有加固不具备上线条件

项目部署后，必须进行加固，否则上线存在安全风险，且上线后加固，存在导致重大问题的风险。

没有加固就上线导致的安全事故，将由项目组承担责任。

只部署一个容器，也需要走部署申请流程

服务器上新增部署应用，即使只新增一个nginx容器，也需要走部署申请流程。通过部署申请流程，集成开发会帮助项目组规划哪台服务器上新增容器，保障系统性能和稳定性。

更新应用联系开发负责人，不需要提交部署流程

更新应用（含整包更新），在基础设施支持部门户上已发布了更新操作文档，项目开发负责更新，如项目开发不会操作，可学习文档，或到新点学堂学习。

部署人员部署完系统，不代表项目已经部署完成

部署人员部署完系统，只是系统部署到服务器上，还不具备使用条件，需经过集成配置、安全加固，直到通过项目组验收才算部署完成。

没有立项、没有可用预算项目，无法部署

没有立项，没有可用预算的项目，无法进行部署。没有立项项目可联系商务进行临时立项，没有可用预算项目，需要申请预算，满足条件后提交部署流程进行部署。

特殊情况需部署，项目组发邮件给营销指导中心（未立项），项目指导中心（无可用预算），经中心负责人邮件反馈后，由集成开发在邮件中反馈规划清单，基础支撑按反馈规划清单进行部署。

项目部署后报错，不是先找基础支撑

按公司产品验证规范，部署的项目部署包应验证通过，项目部署后报错，按如下步骤确认：

- 1、联系集成开发确认有无进行集成配置
- 2、联系项目开发分析日志，如项目开发无法分析日志，联系产品开发/集成开发进行分析。

集成配置后业务系统无法访问，先联系集成开发检查防火墙端口是否开放

按BG对服务器安全加固前置要求（账号密码策略、远程策略、防火墙开通），系统部署阶段部署人员会进行加固（仅负责在系统部署同时进行主机加固，上线后三方检查的漏洞进行主机加固需提交安全知识库给默认处理人），但部分应用因部署包质量、集成配置未完成等因素导致无法启动，进而导致部署阶段安全加固因检测不到在用端口未能加入防火墙端口策略中。

已通过邮件明确由集成开发通过epoint-fence进行操作系统防火墙端口开放。

遇到集成开发反馈不清楚的，可联系BG安全对接人（交易-朱文兵、政务-陆斌、建设-张远阳）。

 关于安全加固前置的说明和防火墙端口开通调整



 OFF 樊斌 于 2024-03-29 11:31 发给 朱文兵、陆斌、张远阳、陆莉军、高龙宇、陈嘉祎、陆仁杰、李昕轶、陈明秀、樊斌、施奕楠、汤胜利、邱蒙恩、陈巧玲、刘建娜、朱伟...

[完整信息](#)

各位领导、同事，

针对2023年各BG安全对接人提出的主机安全加固滞后问题，以及系统部署同时完成主机安全加固的呼声。

2024年3月20日开始，基础设施支持部将主机安全加固前置，由部署人员部署系统同时，完成主机安全加固（通过最新发布的加固工具epoint-fence快速完成防火墙、账号策略管理配置）。

由于主机安全加固前置，业务在仅配置JDBC无法拉起情况下，业务端口未处于监听状态，此时加固工具无法检测到并开通端口可能影响到算法平台部署、集成开发配置。

按BG安全对接人反馈的意见，此类情况需算法平台部署人员和集成开发遇到防火墙端口未开通情况，自行进行端口开通。

1、存量项目在原先服务器上部署应用，基本使用firewalld防火墙，算法平台部署人员或集成开发可使用firewall-cmd命令进行防火墙端口开通。

2、3月20日开始提交部署的新服务器使用epoint-fence管理防火墙端口，服务器上无firewall-cmd命令，算法平台部署人员或集成开发需使用epoint-fence开通防火墙端口。

FAQ-基础设施支持门户

The screenshot shows the Epoint portal interface. On the left, a sidebar menu has '中研院门户' (Institute Portal) highlighted under the '技术门户' (Technology Portal) category. A red arrow points from this menu item to the '中研院技术门户' (Institute Technology Portal) page. In this page, the '支持与服务' (Support & Service) tab is selected, and within it, the '基础设施支持中心' (Infrastructure Support Center) is highlighted. Below this, a table of contents for the '基础设施支持部对外服务清单划分' (Infrastructure Support Department External Service List Division) is shown, with the first five chapters (Department Division, Servers, Product Deployment, Project Updates, and Project Inspection & Reinforcement) enclosed in a red box. At the bottom, a table titled '2021-9' shows the division of work.

基础设施支持部对外服务清单划分

2021-9

工作分类	工作环节	具体工作内容	责任部门
	部署排队	插队项目审核, 调整排队顺序	集成开发/产品线

- 基础设施支持部门户在OA可以找到。
- 基础设施支持部部门门户列出了部门的分工和沟通渠道；操作系统安装；产品部署和更新；巡检和加固处理；以及常见问题的处理等内容。

FAQ-磁盘性能、CPU、内存检测

```
{
  "rndrd":"13209.28",
  "rndwr":"10139.95",
  "seqrd":"14061.18",
  "seqrewr":"19904.99",
  "seqwr":"9895.11",
  "seqwr_4":"9278.06",
  "seqwr_1":"9919.41",
  "fio_write":"21.8k",
  "fio_write_16":"20.9k",
  "fio_read":"25.5k",
  "fio_read_16":"24.8k"
}
```

删除了原来服务器的推荐值

仅给出测试值本身，判断是否合适本项目，由集成开发根据项目规模进行判断

说明：为了获得磁盘本身性能，并贴近真实的文件读写场景，fio主要参数为 ioengine=psync fallocafe=none bs=8k
当三方使用 -ioengine=libaio参数时，实际测试的是linux内核和磁盘之间的异步IO性能，可以理解为应用程序拿内核做文件读写的缓存，并非实际的磁盘性能
java原生的文件读写操作默认无法使用libaio，因此当fio使用该参数获得很高的IO性能时，只能表示linux内核对异步IO优化的很好，对java默认的文件读写操作没有帮助。

—*— 本机IP信息：

ens192 : 192.168.1.1

docker0 : 172.17.0.1

OS: CentOS Linux release 7.9.2009 (Core) 3.10.0-1160.53.1.el7.x86_64

CPU: Intel(R) Xeon(R) Gold 6278C CPU @ 2.60GHz x 4

MEM: 8G

PKG: 376

DISK:

Filesystem	Size	Used	Avail	Use%	Mounted on
devtmpfs	3.9G	0	3.9G	0%	/dev
tmpfs	3.9G	0	3.9G	0%	/dev/shm
tmpfs	3.9G	8.6M	3.9G	1%	/run
tmpfs	3.9G	0	3.9G	0%	/sys/fs/cgroup
/dev/vda1	40G	2.4G	35G	7%	/
tmpfs	783M	0	783M	0%	/run/user/0
/dev/vdb1	50G	17G	34G	33%	/media

NAME	MAJ:MIN	RM	SIZE	RO	TYPE	MOUNTPOINT
vda	253:0	0	40G	0	disk	
└─vda1	253:1	0	40G	0	part	/
vdb	253:16	0	50G	0	disk	
└─vdb1	253:17	0	50G	0	part	/media

磁盘性能、CPU、内存检测，最新版本的sysbench bin包支持一次检测展示所有结果。

- 磁盘IOPS检测结果
- 显示了操作系统和内核版本
- 显示了CPU型号、核心数
- 显示了内存容量
- 显示了磁盘大小和分区

磁盘检测在线操作文档：

https://fdoc.epoint.com.cn:3366/epoint_deploy_book/Product_deploy/Know/envprepare/Disk_Check.html

FAQ-端口检测

```
[root@VM-4-14-centos mittest]# ./probeporttest -s -c -A -H 127.0.0.1
Server is preparing, please wait ...
tcp - 0.0.0.0:443 status: already listened(success)!
udp - 0.0.0.0:443 status: already listened(success)!
tcp - 0.0.0.0:8080 status: already listened(success)!
udp - 0.0.0.0:8080 status: already listened(success)!
tcp - 0.0.0.0:80 status: already listened(success)!
udp - 0.0.0.0:80 status: already listened(success)!
```

Client output:

```
tcp - 127.0.0.1:443 status:open(success)!
udp - 127.0.0.1:443 status:open(success)!
tcp - 127.0.0.1:8080 status:open(success)!
udp - 127.0.0.1:8080 status:open(success)!
tcp - 127.0.0.1:80 status:open(success)!
udp - 127.0.0.1:80 status:open(success)!
```

```
D:\probeport内测版端口检测工具>probeporttest.exe -s -c -A -H 127.0.0.1
Server is preparing, please wait ...
```

```
tcp - 0.0.0.0:443 status: already listened(success)!
udp - 0.0.0.0:443 status: already listened(success)!
tcp - 0.0.0.0:8080 status: already listened(success)!
udp - 0.0.0.0:8080 status: already listened(success)!
tcp - 0.0.0.0:80 status: already listened(success)!
udp - 0.0.0.0:80 status: already listened(success)!
```

Client output:

```
tcp - 127.0.0.1:443 status:open(success)!
udp - 127.0.0.1:443 status:open(success)!
tcp - 127.0.0.1:8080 status:open(success)!
udp - 127.0.0.1:8080 status:open(success)!
tcp - 127.0.0.1:80 status:open(success)!
udp - 127.0.0.1:80 status:open(success)!
```

服务器清单上已经列出了所需要的端口，提交部署申请时，需确认服务器端口是否已开通。通常不同网段之间的服务器端口需要申请开通，但存在部分项目同一网段内的服务器之间端口也需要申请开通（例如中石化项目）。服务器之间端口是否已开通，可以通过端口检测工具进行检测。目前较多项目组因端口不通影响系统部署进度。

端口检测在线操作文档：

https://fdoc.epoint.com.cn:3366/epoint_deploy_book/Product_deploy/Know/envprepare/probeport.html

FAQ-带宽检测

```
[root@Centos7 ~]# cat a1.log
Connecting to host 192.168.223.101, port 5201
[ 5] local 192.168.223.100 port 41232 connected to 192.168.223.101 port 5201
[ ID] Interval           Transfer     Bandwidth       Retr   Cwnd
[ 5]  0.00-1.00   sec    112 MBytes   942 Mbits/sec    0     209 KBytes
[ 5]  1.00-2.00   sec    118 MBytes   994 Mbits/sec    0     212 KBytes
[ 5]  2.00-3.00   sec    125 MBytes  1.05 Gbits/sec    0     212 KBytes
[ 5]  3.00-4.00   sec    115 MBytes   964 Mbits/sec    0     212 KBytes
[ 5]  4.00-5.00   sec    117 MBytes   985 Mbits/sec    0     212 KBytes
[ 5]  5.00-6.00   sec    123 MBytes  1.04 Gbits/sec    0     212 KBytes
[ 5]  6.00-7.00   sec    117 MBytes   984 Mbits/sec    0     212 KBytes
[ 5]  7.00-8.00   sec    124 MBytes  1.04 Gbits/sec    0     212 KBytes
[ 5]  8.00-9.00   sec    119 MBytes  1.00 Gbits/sec    0     212 KBytes
[ 5]  9.00-10.00  sec    113 MBytes   945 Mbits/sec    0     212 KBytes
- - - - -
[ ID] Interval           Transfer     Bandwidth       Retr
[ 5]  0.00-10.00  sec   1.16 GBytes   994 Mbits/sec    0             sender
[ 5]  0.00-10.00  sec   1.16 GBytes   994 Mbits/sec                  receiver

iperf Done.
```

检测结果为：网络带宽994Mb /秒，客户端与服务端之间网络符合千兆要求。

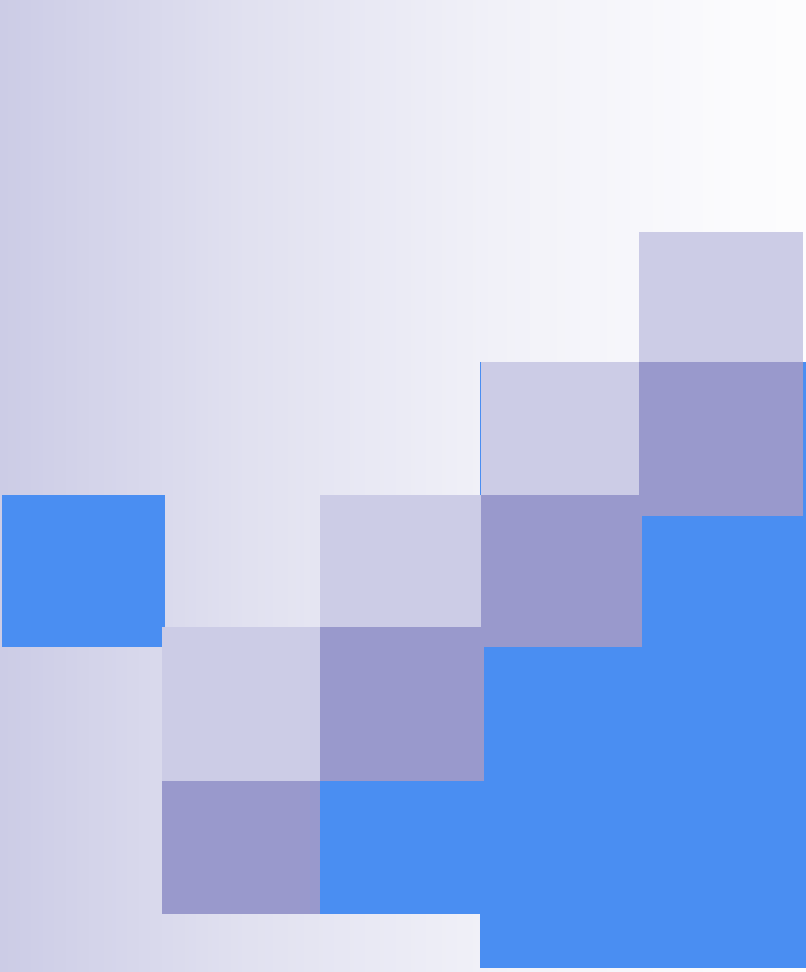
交易项目涉及投标文件上传、解密等操作，且投标文件较大，对网络带宽要求更高，要求服务器之间网络带宽满足千兆要求。因此需要进行带宽检测。

带宽检测在线操作文档：

https://fdoc.epoint.com.cn:3366/epoint_deploy_book/Product_deploy/Know/envprepare/iperf.html

最新部署规范近期将发布，根据交付侧要求，增加了项目部署暂停原因分析和追责部分，属于项目组准备不足导致的暂停，交付侧将安排浮动处理。

最新迁移规范近期将进行评审，目的是通过规范明确迁移范围避免遗漏，明确迁移流程涉及的各责任人，避免联系不到对应人员。



谢谢！