

产品简介



蓝鲸管控平台，是整个蓝鲸平台的底层管控系统，是蓝鲸所有其他服务的基础，是蓝鲸服务体系与用户机器的连接器。

在整个蓝鲸体系中，蓝鲸管控平台作为蓝鲸的底层管控通道，没有提供独立的接口供用户直接访问调用，而是通过蓝鲸 esb 能力向上提供服务，供上层平台或者 SaaS 去实现场景赋能，蓝鲸管控平台主要提供了三种类型的服务能力：**文件传输能力、实时任务执行能力、数据采集与传输的能力**。

术语解释

GSE: 蓝鲸管控平台系统简称 (General Service Engine)。

BK Agent: 蓝鲸智能 Agent，部署在业务服务器上的代理程序。

BK TaskServer: 蓝鲸管控平台任务及控制服务端程序。

BK FileServer: 蓝鲸管控平台文件传输控制服务端程序。

BK DataServer: 蓝鲸管控平台数据传输服务端程序。

BK DB Proxy: 蓝鲸管控平台 Redis 集群管理模块。

BK ApiServer: 蓝鲸管控平台提供外部 api 的服务程序。

BK AlarmServer: 蓝鲸管控平台告警服务程序。

BK ProcServer: 蓝鲸管控平台进程与配置管理服务程序。

BK ProcMgrServer: 蓝鲸管控平台进程管理服务程序。

BK SyncDataServer: 蓝鲸管控平台数据同步服务程序。

BK DataOpServer: 蓝鲸管控平台数据传输服务运营监控程序。

BK TransitServer: 蓝鲸管控平台跨云数据转发程序。

BK OperServer: 蓝鲸管控平台 ping 告警服务程序。

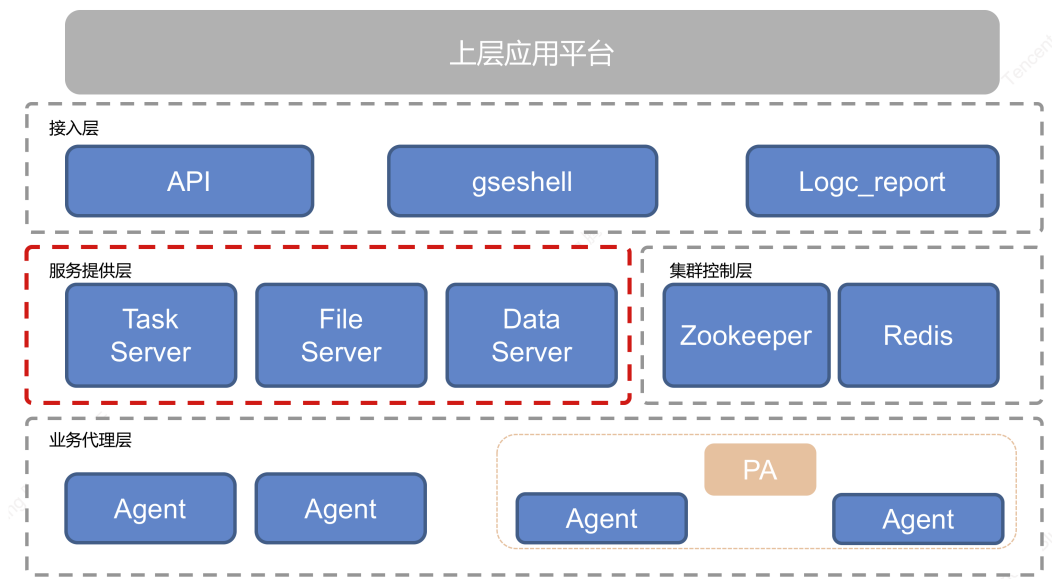
BK OperTransServer: 蓝鲸管控平台 ping 不可达检测程序。

Redis: 一种基于内存的 Key-Value 数据库。

Zookeeper: 一种分布式应用程序协调服务。

Thrift: 一种跨语言的进程间通信协议。

产品架构图



从网络框架层面来看，蓝鲸管控平台分为两层网络架构，分别为 **服务层** 和 **业务代理层**，服务层

由三种不同类型的服务集群构成：控制任务执行的 TaskServer 集群、负责数据采集传输服务的 DataServer 集群以及提供文件高速传输服务的 FileServer 集群，业务代理层则是部署在业务服务器上的蓝鲸Agent，承载了服务层提供的三种服务。

Agent: 蓝鲸智能 Agent，可以安装在业务需要管控的 **实体机、虚拟机或者容器里面**，BK Agent 是蓝鲸管控平台提供三大服务能力的实际执行者。

PA: 蓝鲸管控平台跨云代理节点，为云区域 BK Agent 提供代理转发服务，提供跨云区域机器管控能力。

TaskServer: 蓝鲸管控平台任务及控制服务端程序，该程序提供对集群内 Agent 的管理能力，并支持对 Agent 批量下发和执行发命令或脚本。

FileServer: 蓝鲸管控平台文件传输控制服务端程序，该程序对指定范围内 Agent 节点提供 BT 种子服务，保证对传输的安全性、不同区域及业务模块间的隔离性，并控制 BT 传输在有限的贪婪特性范围内。

DataServer: 蓝鲸管控平台数据传输服务端程序，该服务端主要提供对 Agent 采集的数据进行汇聚、分类、流转能力。对于普通的千兆网卡机器，BK DataServer 能够提供百兆级别的数据处理能力。

Redis: Redis 在本系统中提供工作区数据缓存作用。

Zookeeper: Zookeeper 主要提供对集群的管理能力，包括集群中不同节点间的相互发现，有效性探测等。

支持 OS 类型

OS 类型	主要 OS 版本
CentOS	5.8 32/64 位
	5.11 32/64 位
	6.x 32/64 位
	7.x 32/64 位
Redhat	6.x 32/64 位
	7.x 32/64 位
Debian	7.4 64 位
SUSE	10 64 位
Ubuntu	14.04 32/64 位
	10.04 32/64 位
	12.04 64 位
	2012

Windows Server	2008
	2003
	Win 7
AIX (企业版)	AIX 6
	AIX 7
linuxone	IBM Linuxone 64 位
linux-arm	华为arm服务器linux 64 位

文件传输

文件传输是指用户从指定机器将指定文件批量传输到特定范围的机器上，文件传输具备以下几个特性。

传输模式

BT模式：对于大于 10KB 的文件，蓝鲸管控平台将自动启用 BT 作为首选的传输方式。

直传模式：对于 10KB 以下的小文件，将使用 tcp 直传模式。

混合模式：在 BT 模式下，如果发生 BT 传输持续性失败，则会尝试使用直传模式传输 BT 文件分片，当 BT 传输恢复时，则自动切换至 BT 模式。

传输类型

文件传输：分发单个文件到指定机器，这里文件可以是任何格式，任何可读目录下的可读文件；文件分发完成后，会自动同步目标文件权限与源文件一致；对于直传模式，文件传输结束后会进行 MD5 校验，对于 BT 模式和混合模式，会进行 hash 值校验文件的完整性。

目录传输：用户可以将指定目录传输到一批机器的指定可写目录下，目录传输将保持目录的结构和权限不变。

正则匹配传输：用户可以通过通配符（符合通用正则表达式）匹配一批文件，并传输到指定机器的指定可写目录，传输完成后文件的格式和权限与源文件保持一致。

传输控制

区域链控制：让文件沿着指定的路径，通过多个中转节点的接力，最终到达目标机器，并且源文件和目标文件所在机器不在同一个物理或逻辑区域，我们称这种传输方式为区域链传输。区域链控制是指通过一定规则指定文件中转的路径，以满足具有特殊专线链接的两个区域间的传输需求。

跨区域穿透：跨区域穿透是指原本相互隔离的两个区域，由于特殊目的，需要就本次传输进行定向透传。蓝鲸管控平台允许权限用户适当修改配置来完成这种定向穿透。

实时任务执行

蓝鲸管控平台采用分布式多层级任务控制机制，实现海量多层级联网络的主机管控。

支持的任务类型

命令类型：支持 Linux 的 Bash 命令、Windows 的 CMD 命令，支持各种自定义可执行文件格式程序的启动，支持各种解释性语言程序的执行。

脚本类型：支持 Shell、Python、PowerShell、Perl、Bat 等解释性语言脚本。

任务控制方式

指定用户执行：Linux 及其他类 Linux 系统支持按指定用户执行任务，例如用户设定以 user 用户执行 ps，则只能看到该用户权限范围内的结果；因为 Windows 操作系统的限制，只有开启校验机器密码功能的用户才能指定用户执行任务，否则都以 SYSTEM 用户执行任务。

继承用户环境：Linux 及其他类 Linux 系统支持指定用户后继承该用户设定的环境变量，Windows 无此功能。

有害操作告警：蓝鲸管控平台能够对高危操作进行预警，高危操作的定义由系统自动设定。

有害操作防护：蓝鲸管控平台能够对高危操作进行预警并干预，高危操作的定义及干预措施提供选项供用户配置。

数据采集与传输

采集方式

自定义数据采集：Agent 开放数据发送接口，供用户开发自定义的数据采集程序或脚本。

采集器插件化支持：Agent 支持采集器插件化，自动加载采集插件，并监控插件的存活状况。如果采集插件异常终止，则重新拉起采集插件；如果多次拉起失败则会触发告警。

实时数据快照：管控平台支持缓存安装有 Agent 的机器 1min 内的系统快照数据，并提供接口供用户访问。

传输控制

动态负载均衡：由于 Agent 数据采集的量较大，且具有随业务特性波动的特点，这些数据在流转时需要高性能的服务端做收敛转发，为了提供服务端机器的利用率，减少由于数据量变化时带来的负载不均衡问题，管控系统支持按分钟级别动态调整数据转发的通道，以达到集群内服务端负载均衡的目的。

集群管理

蓝鲸管控平台提供了一套有效的集群管理机制，让整个任务负载处理更加智能。

自动服务发现

同一个集群内的模块均支持自动发现，用户扩缩容任何节点，系统均能实时感知，并调整通讯策略，保证服务的高可用。

集群负载均衡

同一个集群内，支持按照 Agent 链接数进行负载均衡。

Agent 状态查询

蓝鲸管控平台提供接口，查询 Agent 状态。接口按照实时性分为两类：一类为实时状态接口，只能查询当前 Agent 是否正常；二类接口提供24s内的状态查询，查询的内容包括 Agent 上次心跳时间、Agent 版本、Agent 使用的 cpu、Agent 使用的 mem。

Agent 失连告警

蓝鲸管控平台会监控 Agent 的心跳，心跳失连的 Agent 信息会通过告警的方式及时通知用户。

多区域负载均衡

蓝鲸管控平台支持对同一集群进行不同区域的划分，不同区域按照各区域内的负载均衡规则处理；未划分区域的 Agent 按照集群负载均衡策略处理。

蓝鲸管控平台 API 简介

资源名称	资源描述
get_agent_info	Agent 心跳信息查询

资源名称	资源描述
get_agent_status	Agent 在线状态查询

请求地址

/api/c/compapi/v2/gse/get_agent_info/

请求方法

POST

功能描述

查询 agent 心跳详细信息。数据非实时，延时1分钟内。

请求参数

通用参数

字段	类型	必选	描述
bk_app_code	string	是	应用 ID
bk_app_secret	string	是	安全密钥(应用 TOKEN)，可以通过 蓝鲸智云开发者中心 -> 点击应用 ID -> 基本信息 获取
bk_token	string	否	当前用户登录态，bk_token 与 bk_username 必须一个有效，bk_token 可以通过 Cookie 获取
bk_username	string	否	当前用户用户名，应用免登录态验证白名单中的应用，用此字段指定当前用户

接口参数

字段	类型	必选	描述
bk_supplier_account	string	是	开发商账号
hosts	array	是	主机列表

HOSTS

字段	类型	必选	描述
bk_cloud_id	int	是	云区域 ID
ip	string	是	IP 地址

请求参数示例

```
{
  "bk_app_code": "esb_test",
  "bk_app_secret": "xxx",
  "bk_token": "xxx",
  "bk_supplier_account": "0",
  "hosts": [
    {
      "ip": "10.0.0.1",
      "bk_cloud_id": 0
    }
  ]
}
```

```
]
}
```

返回结果示例

```
{
  "result": true,
  "code": 0,
  "message": "",
  "data": {
    "0:10.0.0.1": {
      "ip": "10.0.0.1",
      "version": "V0.01R060D38",
      "bk_cloud_id": 0,
      "parent_ip": "10.0.0.2",
      "parent_port": 50000
    }
  }
}
```

返回结果参数说明

DATA

字段	类型	描述
key	string	格式为：bk_cloud_id:ip
value.ip	string	主机 IP 地址
value.bk_cloud_id	int	云区域 ID
value.version	string	agent 版本号
value.parent_ip	string	agent 的上级节点 ip
value.parent_port	int	agent 的上级节点端口

请求地址

/api/c/compapi/v2/gse/get_agent_status/

请求方法

POST

功能描述

查询 agent 实时在线状态

请求参数

通用参数

字段	类型	必选	描述
bk_app_code	string	是	应用 ID

字段	类型	必选	描述
bk_app_secret	string	是	安全密钥(应用 TOKEN)，可以通过 蓝鲸智云开发者中心 -> 点击应用 ID -> 基本信息 获取
bk_token	string	否	当前用户登录态，bk_token 与 bk_username 必须一个有效，bk_token 可以通过 Cookie获取
bk_username	string	否	当前用户用户名，应用免登录态验证白名单中的应用，用此字段指定当前用户

接口参数

字段	类型	必选	描述
bk_supplier_account	string	是	开发商账号
hosts	array	是	主机列表

HOSTS

字段	类型	必选	描述
bk_cloud_id	int	是	云区域 ID
ip	string	是	IP 地址

请求参数示例

```
{
  "bk_app_code": "esb_test",
  "bk_app_secret": "xxx",
  "bk_token": "xxx",
  "bk_supplier_account": "0",
  "hosts": [
    {
      "ip": "10.0.0.1",
      "bk_cloud_id": 0
    }
  ]
}
```

返回结果示例

```
{
  "result": true,
  "code": 0,
  "message": "",
  "data": {
    "0:10.0.0.1": {
      "ip": "10.0.0.1",
      "bk_cloud_id": 0,
      "bk_agent_alive": 1
    }
  }
}
```

返回结果参数说明

DATA

字段	类型	描述
key	string	格式为: bk_cloud_id:ip
value.ip	string	主机 IP 地址
value.bk_cloud_id	int	云区域 ID
value.bk_agent_alive	int	agent 在线状态, 0 为不在线, 1 为在线

常见问题

通过 JOB 执行任务报错 “GSE SERVER FAILED”

- (1) 检查 gse_task 进程状态是否正常
- (2) 检查 gse_task 是否正常监听 48669 端口
- (3) 检查作业平台和管控平台的证书是否匹配
- (4) 检查作业平台部署主机到管控平台部署主机的 48669 端口策略是否开通
- (5) 检查 gse.service.consul 是否解析正常

通过作业平台执行任务报错 “can not find agent by ip ...”

- (1) 检查对应 ip 机器上的 gse_agent 是否正常
- (2) 检查 gse_agent 的 48668 连接是否正常
- (3) 检查 gse_agent 与 gse_task 的证书是否匹配
- (4) 检查该 ip 在配置平台上的业务及云区域 id 是否正确

文件传输任务超时失败

- (1) 根据作业平台打屏信息, 判断是上传还是下载超时
- (2) 检查 bt 传输的端口策略是否开通

点管理 SaaS 或作业平台显示 Agent 异常

- (1) 检查对应 ip 机器上的 gse_agent 是否正常
- (2) 检查 gse_agent 的 48668 连接是否正常

(3) 检查 gse_agent 与 gse_task 的证书是否匹配

(4) 检查该 ip 在配置平台上的业务及云区域 id 是否正确

(5) 若以上检查结果均正常，检查 gse_api 日志是否有 “no db proxy server addr found” 报错，若有则重启 gse_api

通过作业平台重启 gse_agent 环境变量不生效

- 问题现象

安装 python 后，添加 python 环境变量，通过 `restart.bat` 脚本重启 Agent 后环境变量不生效。

- 问题原因

通过作业平台执行 Agent，环境变量是不会生效的，因为环境变量是基于当前上下文环境的，通过 Agent 重启时，Agent 上本身没有最新的环境变量信息，所以也不会生效。

- 解决方案

需要在能获取到最新环境变量的状态下重启 gseagent，比如登录到机器重启 gse_agent 进程。

PA 机器上的 Agent 显示未安装

- 问题现象

手动安装 proxy，主机监控数据上报正常，p-agent 数据及 agent 状态也正常，但是 proxy 这台代理服务器在主机监控及作业平台均显示 agent 未安装。通过 JOB 执行任务报错，提示 agent 未安装。

- 问题原因

有些用户的机器连接 gse server 时看到的 ip 和本机 ip 不一致，做了 NAT 转换，所以 agent 安装部署时导入 cmdb 的 ip 使用 identityip 作为标识。proxy 上的 agent 实际在本机建立连接，未经过 nat 转换，所以实际通信的 ip 就是本机真实 ip。

- 解决方案

- 在 cmdb 上导入 agentip 中配置的 ip。

- 两台 proxy 情况，建议这种网络情况下，交叉配置另一台 proxy 的 ip，这种就可以统一用 identityip 在 cmdb 中导入。