开通策略

日志中台主机: 10.129.8.187, 10.129.8.188, 10.129.8.189

端口: 515-520 tcp, udp

安装方式

1.配置需要采集的目录文件

参见filebeat.yml文件对应部分

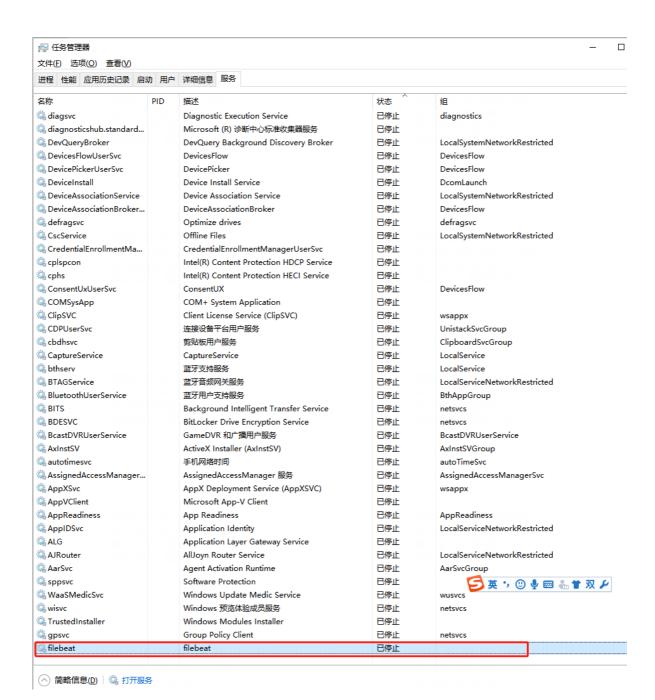
2.配置日志中台的接收地址

参见filebeat.yml文件对应部分

3.启动

```
#前台启动(用于测试)
.\filebeat.exe -c filebeat.yml -e

#后台启动
#1.进入filebeat_windows的安装目录下,打开powershell
#2.执行(会将filebeat安装成为一个服务)
powershell.exe -ExecutionPolicy UnRestricted -File .\install-service-filebeat.ps1
```



启动filebeat服务(右键,选择"开始")

BITS	Background Intelligent Transfer Service	已停止	netsvcs	
A BDESVC	BitLocker Drive Encryption Service	已停止	netsvcs	
BcastDVRUserService	GameDVR 和广播用户服务	已停止	BcastDVRUserService	
AxInstSV	ActiveX Installer (AxInstSV)	已停止	AxInstSVGroup	
autotimesvc	手机网络时间	已停止	autoTimeSvc	
Assigned Access Manager	AssignedAccessManager 服务	已停止	AssignedAccessManagerSvc	
AppXSvc	AppX Deployment Service (AppXSVC)	已停止	wsappx	
AppVClient	Microsoft App-V Client	已停止		
AppReadiness	App Readiness	已停止	AppReadiness	
AppIDSvc	Application Identity	已停止	LocalServiceNetworkRestricted	
ALG	Application Layer Gateway Service	已停止		
AJRouter	AllJoyn Router Service	已停止	LocalServiceNetworkPostcietod	
AarSvc	Agent Activation Runtime	已停止	AarSvcGroup 开始(S)	
sppsvc	Software Protection	已停止	⊝英 , 停止(П)	
₩aaSMedicSvc	Windows Update Medic Service	已停止	wusvcs 重新启动(R)	
wisvc	Windows 预览体验成员服务	已停止	netsvcs 打开服务(V)	
TrustedInstaller	Windows Modules Installer	已停止	在线搜索(O)	
gpsvc	Group Policy Client	已停止	netsvcs 转到详细信息(D)	
्र filebeat	filebeat	已停止	44937779	