

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
```

任务管理器				
文件(F) 选项(O) 查看(V)				
进程 性能 应用历史记录 启动 用户 详细信息 服务				
名称	PID	描述	状态	组
diagsvc		Diagnostic Execution Service	已停止	diagnostics
diagnosticshub.standard...		Microsoft (R) 诊断中心标准收集器服务	已停止	
DevQueryBroker		DevQuery Background Discovery Broker	已停止	LocalSystemNetworkRestricted
DevicesFlowUserSvc		DevicesFlow	已停止	DevicesFlow
DevicePickerUserSvc		DevicePicker	已停止	DevicesFlow
DeviceInstall		Device Install Service	已停止	DcomLaunch
DeviceAssociationService		Device Association Service	已停止	LocalSystemNetworkRestricted
DeviceAssociationBroker...		DeviceAssociationBroker	已停止	DevicesFlow
defragsvc		Optimize drives	已停止	defragsvc
CscService		Offline Files	已停止	LocalSystemNetworkRestricted
CredentialEnrollmentMa...		CredentialEnrollmentManagerUserSvc	已停止	
cplspcon		Intel(R) Content Protection HDCP Service	已停止	
cphs		Intel(R) Content Protection HECI Service	已停止	
ConsentUxUserSvc		ConsentUX	已停止	DevicesFlow
COMSysApp		COM+ System Application	已停止	
ClipSVC		Client License Service (ClipSVC)	已停止	wsappx
CDPUserSvc		连接设备平台用户服务	已停止	UnistackSvcGroup
cbdhsvc		剪贴板用户服务	已停止	ClipboardSvcGroup
CaptureService		CaptureService	已停止	LocalService
bthserv		蓝牙支持服务	已停止	LocalService
BTAGService		蓝牙音频网关服务	已停止	LocalServiceNetworkRestricted
BluetoothUserService		蓝牙用户支持服务	已停止	BthAppGroup
BITS		Background Intelligent Transfer Service	已停止	netsvcs
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
AssignedAccessManager...		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	LocalServiceNetworkRestricted
AarSvc		Agent Activation Runtime	已停止	AarSvcGroup
sppsvc		Software Protection	已停止	
WaaSMedicSvc		Windows Update Medic Service	已停止	wusvcs
wisvc		Windows 预览体验成员服务	已停止	netsvcs
TrustedInstaller		Windows Modules Installer	已停止	
gpsvc		Group Policy Client	已停止	netsvcs
filebeat		filebeat	已停止	

启动filebeat服务(右键, 选择“开始”)

BITS	Background Intelligent Transfer Service	已停止	netsvcs
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
AssignedAccessManager...	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	LocalServiceNetworkRestricted
AarSvc	Agent Activation Runtime	已停止	AarSvcGroup
sppsvc	Software Protection	已停止	
WaaSMedicSvc	Windows Update Medic Service	已停止	wusvcs
wisvc	Windows 预览体验成员服务	已停止	netsvcs
TrustedInstaller	Windows Modules Installer	已停止	netsvcs
gpsvc	Group Policy Client	已停止	netsvcs
filebeat	filebeat	已停止	

