

Elasticsearch Service Beats 指南







【版权声明】

©2013-2025 腾讯云版权所有

本文档(含所有文字、数据、图片等内容)完整的著作权归腾讯云计算(北京)有限责任公司单独所有,未经腾讯云事先明确书面许可,任何主体不得以任何形式 复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯,腾讯云将依法采取措施追究法律责任。

【商标声明】

🔗 腾讯云

及其它腾讯云服务相关的商标均为腾讯云计算(北京)有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标,依法由权利人所有。未经腾讯云及有关 权利人书面许可,任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为,否则将构成对腾讯云及有关权利人商标权的侵犯,腾讯云将依 法采取措施追究法律责任。

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况,部分产品、服务的内容可能不时有所调整。 您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定,除非双方另有约定,否则,腾讯云对本文档内容不做任何明示或默示的承 诺或保证。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务,及相应的技术售后服务,任何问题请联系 4009100100或95716。



文档目录

Beats 指南

概述

角色授权

采集 CVM 数据

创建 Filebeat 采集日志文件

创建 Metricbeat 采集系统数据

创建 Auditbeat 采集审计数据

创建 Heartbeat 采集服务器状态 创建 Packetbeat 采集网络流量

管理 CVM 实例

通过 Filebeat 采集 TKE 容器日志



Beats 指南 概述

最近更新时间: 2024-10-30 17:12:01

腾讯云 Beats 是基于开源的轻量数据采集器平台 Beats 构建的云端托管服务,提供自动化的 Beats 采集器配置下发服务,支持采集 CVM 服务数据,并发送 到腾讯云 ElasticSearch 集群或 Logstash 实例。

工作方式

腾讯云 Beats 能够采集 CVM 服务日志、指标、服务器状态、审计日志、网络流量等多种事件数据,支持的采集器类型如下:

采集器名称	简介	文档
Filebeats	日志采集器,用于收集和传送日志文件	创建 Filebeat 采集日志文件
Metricbeats	指标采集器,输送系统和服务统计数据	创建 Metricbeat 采集系统数据
Auditbeats	审计数据采集器,收集 Linux 审计框架数据	创建 Auditbeat 采集审计数据
Heartbeats	运行状态监测数据采集器,可以主动探测服务的可用性	创建 Heartbeat 采集服务器状态
Packetbeats	网络流量采集器,用于应用程序和性能监测	创建 Packetbeat 采集网络流量

可以将数据发送到腾讯云 Elasticsearch 或 Logstash 中进一步处理,然后在 Kibana 中可视化。



特点与优势

- 简化操作,方便部署和管理。
- 集成官方多种采集器类型。



角色授权

最近更新时间:2024-10-3017:12:01

使用 Beats 服务时,需要您为 ES 服务账号授予服务相关角色 ES_QCSLinkedRoleInBeatsCollector,腾讯云 ES 才能访问您账号下的"自动化助手服 务"来下发 Beats 配置到 CVM 并采集数据源日志。此权限无须主动寻找和配置,在使用 Beats 过程中,涉及此授权时,系统默认出现授权界面。 本文介绍腾讯云 ES 服务相关角色 ES_QCSLinkedRoleInBeatsCollector 的授权场景,以及如何删除服务相关角色。

授权场景

当您已注册并登录腾讯云账号后,首次创建 Beats 服务时,腾讯云 ES 将自动创建具有执行任务权限的角色,并默认出现授权界面,引导您跳转**访问管理**页面, 对当前角色授予操作云服务器(CVM)、腾讯云自动化助手(TAT)等其他云资源的权限。腾讯云 ES 通过扮演该角色,即可调用相关 API,完成 Beats 采集 器在 CVM 机器上的数据采集任务。

△ 注意

首次使用 Beats 服务时,主账号需要完成角色授权流程,授权后子账号无需额外进行角色授权,但是子账号需要有 CVM 云服务的 DescribeInstances 接口的权限、CAM 访问管理的 PaasRole 接口的权限、TAT 自动化助手的 DescribeAutomationAgentStatus 接口的权 限。

授权流程

1. 登录 Elasticsearch Service 控制台 Beats 管理,当用户首次使用 Beats 服务时,会有如下提示。单击前往授权进行角色授权。



2. 在跳转页面中,单击同意授权,将服务相关角色 ES_QCSLinkedRoleInBeatsCollector 授予腾讯云 ES 的服务账号。



3. 授权完成后,用户需刷新腾讯云 ES 的控制台,刷新后即可正常操作。更多 ES_QCSLinkedRoleInBeatsCollector 相关的详细策略信息,可在授权后登录访问管理控制台查看。

权限内容

预设策略:



策略名称	权限说明
QcloudAccessForESLinkedRol	该策略仅供腾讯云 Elasticsearch Service(ES)服务相关角色
eInBeatsCollector	(ES_QCSLinkedRoleInBeatsCollector)进行关联,用于 ES 访问其他云服务资源

删除角色

删除 ES_QCSLinkedRoleInBeatsCollector 服务相关角色,需要先删除依赖这个服务相关角色的所有 Beats 采集器。角色删除后,支持在腾讯云 ES 控 制台再次授权。

删除服务相关角色的具体操作,可参见 删除角色。

采集 CVM 数据 创建 Filebeat 采集日志文件

最近更新时间: 2024-10-12 21:50:12

腾讯云

对于需要采集并分析腾讯云 CVM 服务日志的场景,可以使用 Filebeat 采集数据,再发送到腾讯云 Logstash 中进行过滤与预处理,最终传输到腾讯云 Elasticsearch 集群中进行存储,之后可以在 Kibana 中查询并分析日志。本文介绍如何配置 Filebeat 采集部署在腾讯云 CVM 中的服务日志。

应用场景

Filebeat 是一个轻量型的日志采集器,可以轻松地采集云上的 CVM 的日志,从而使得查询或者分析业务服务端的日志变得简单。

- Filebeat 能够逐行读取并发送日志,支持在出现中断的情况下,记录中断时读取到的文件位置信息,后续恢复正常后可以从中断前停止的位置继续开始。
- Filebeat 非常适合采集 nginx、apache 以及容器服务的日志,并且提供可以直接引用的配置模板,极大的简化了这类服务的日志采集过程。

操作须知

1. 腾讯云 CVM 实例、腾讯云 ES 集群和 Logstash 实例,必须在同一 VPC 下。且腾讯云 ES 集群和 Logstash 实例的大版本相同。

▲ 注意 Beats 目前仅支持64位的 Linux 操作系统。

2. 腾讯云 CVM 实例必须安装自动化助手,仅支持为已安装自动化助手的 CVM 实例下发采集器配置。具体操作参见 安装自动化助手客户端 。

操作步骤

Filebeat 采集器配置

1. 登录 Elasticsearch Service 控制台 Beats 管理界面,授权服务相关角色,创建采集器中单击 Filebeat > CVM 日志采集。

Elasticsearch Service	Beats 管理 💿 广州 👻					
日 概況 Sanuariase 無学		① 对于CVM实例,当前只支持采集Linux系统。	,且CVM实例必须配置腾讯云自动化助手环境。 <u>會看</u>	記雲崩南 亿		
前日志分析		创建采集器	1			
PaaS 模式		Filebeat	(Metricbeat	Auditbeat	Heartbeat	Packetbeat
三 ES 集群管理 え ES 索引管理		経動的日本采集時、用于改集和侍达日 + ウル CVM日志采集 TKE日志采集	经量型描标采集器,用于从系统和股务 收集指标	轻量型审计日志采集器,用于收集 Linux 审计框架的数据	面向巡行状态监测的经量型采集器,通过主动探测来监测服务的可用性	经量型网络数据采集器,监测网络流 量,有助于提准网络性能和安全性
@ 数据接入管理		支持強素采集器(D / 采集器名称 / ES集閉ID / Logst	ash宾例D / CKafka宾例ID / Serverless 索引名称	Q	¢	
Beats 管理		采集器(D)名称 # 状态 采集器类型	目▼ 采集器来源 ▼	采集器输出 版本	创建/变更时间	操作

- 2. 在创建 Filebeat 采集器中,设置采集器信息。
- 配置 Filebeat 采集器,输入或选择采集器配置信息。完成后单击下一步。
 - 采集器名称:自定义采集器的名称,格式为1 50个英文、汉字、数字或下划线(_)。
 - 安装版本: 支持6.8.15、7.10.2或7.14.2版本。
 - 采集器输出:采集的数据支持传送到腾讯云 Elasticsearch 集群与 Logstash 实例,请选择与需采集数据的 CVM 在同一 VPC 下的 ES 集群和 Logstash 实例。不支持输出至开源版 ES 集群。
 - 用户名密码:若选择输出采集数据到开启用户登录认证的 ES 集群,需要填写用户名和密码,使得 Filebeat 有权限向 ES 集群中写入数据。用户名默认 为 elastic,密码为集群创建时设置。
 - Monitoring:勾选后生成监控 Filebeat 的相关指标。当采集器输出为 ES 集群时,Monitoring 默认使用和采集器输出相同的 ES 集群;当采集器输 出为 Logstash 实例时,则需要在配置文件中额外添加用于存储监控数据的 ES 集群地址。
 - Kibana Dashboard:勾选后生成默认的 Kibana Dashboard。
 - 采集器 YML 配置: 配置内容如下,更多 YML 配置请参考官方文档 Configure input。
 - type:输入类型,默认为 log,还有 tcp、syslog、stdin 等可选。
 - paths:日志文件路径,需要填写为 CVM 中日志文件的绝对路径。



○ enabled: 是否启用该 input 配置, true 为启用, false 则为不启用。

1 配置Filebeat采	集器 〉 ② 将采集器安装到CVM实例	~
采集器名称 *	长度为1-50,仅支持数字、字母、汉字、-、下划线	
安装版本 *	请选择 ▼	
	安装版本需要和采集器输出的大版本相同	
采集器输出 *	elasticsearch 🔹 请选择 🔹 🗘 新建ES集群 🗹	
	不支持輸出到开源版ES集群	
用户名密码 *	elastic 请填写密码	
启用 Monitoring		
启用 Kibana Dashboard		
采集器YML配置		
filebeat.yml		
1 # ======	Filebeat inputs	
2 3 filebeat.	inputs:	
4 - type:]	og	
5 # Chang	e to true to enable this input configuration.	
6 enabled	: true	
/ # Paths	that should be crawled and fetched. Glob based paths.	
9 - /v	r/log/*.log	
10 # ======		
11		
	下一步取消	

将采集器安装到 CVM 实例。选择要安装采集器的 CVM 实例,完成后单击确定启用。

○ CVM 必须安装自动化助手,仅支持为已安装自动化助手的 CVM 实例下发采集器配置。



○ 仅支持选择和采集器输出在同一 VPC 下的 CVM 实例进行安装,若无法找到目标 CVM 实例,需要更改采集器输出。

在专有网络 🛈				
安装采集器CVM实例★				
支持搜索CVM实例ID / 实例名称 / 穿	2例标签			Q Ø
CVM实例ID/名称	IP地址	操作系统 🛈	采集器状态	自动化助手 🛈
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
共 43 条		10 ▼ 条/页 🛛 🗸	1	/5页 ▶ ▶

3. 单击确定启用后,跳转到 Beats 采集器管理界面,可以查看 Heartbeat 采集器运行状态,显示"正常"则表示采集器安装成功。支持 修改采集器配置 和 管理 CVM 实例。

Logstash 管道配置

如需将采集的日志数据传送到腾讯云 Logstash 实例,可参考 接收 Filebeat 发送的数据并写入到 Elasticsearch 配置 logstash 管道。

Kibana 查看结果

1. 登录腾讯云 Kibana 控制台。



2. 左侧导航栏单击 Dev Tool,执行下述语句,查看采集成功的数据。

GET filebeat-7.10.2/_search	0 0 0 0 0 0 0 0 0 10 "hits" : { 11 "total" : { 12 "value" : 2418, 13 "relation" : "eq"
	<pre> "mx_score" : 1.0, "hits" : [</pre>
① 说明 filebeat-7.14.2为索引名称。	



创建 Metricbeat 采集系统数据

最近更新时间: 2024-10-12 21:50:12

通过 Metricbeat 采集器,能够采集腾讯云 CVM 上的系统数据(包括 CPU 和内存的利用率、磁盘性能、网络性能等),并基于 Kibana 实现可视化分析。

应用场景

Metricbeat 是一个轻量型的指标采集器,可用于采集系统和服务的指标,例如采集系统的 CPU 和内存监控数据,也可以采集 Redis 或者 Nginx 等服务的监 控数据等。

操作须知

1. 腾讯云 CVM 实例、腾讯云 ES 集群和 Logstash 实例,必须在同一 VPC 下。且腾讯云 ES 集群和 Logstash 实例的大版本相同。

▲ 注意 Beats 目前仅支持 Linux 操作系统。

2. 腾讯云 CVM 实例必须安装自动化助手,仅支持为已安装自动化助手的 CVM 实例下发采集器配置。具体操作参见 安装自动化助手客户端 。

操作步骤

Metricbeat 采集器配置

1. 登录 Elasticsearch Service 控制台 Beats 管理界面,授权服务相关角色,单击创建 Metricbeat 采集器。

Elasticsearch Service	Beats 管理 💿 广州 👻					
吉 概范		⑦ 对于CVM实例,当前只支持采集Linux系统	8、且CVM实例必须配置腾讯云自动化助手环境。查	看記蜜指南 12		
Serverless 穩式						
信 日志分析		创建采集器				
② 实时搜索		0.000				
PaaS 模式		Filebeat	Metricbeat	Auditbeat	Heartbeat	Packetbeat
三 ES 集群管理		经量的日志采集器,用于收集和传达日	轻量型描标采集器,用于从系统和服务	经量型审计日志采集器,用于收集	面向运行状态监测的经量型采集器,通	轻量型网络数据采集器, 监测网络流
°。ES 索引管理		6.XIF	102時5日15	LINUX ID TT 12 RID/SXSW	过主动体测米兰制度分约可用性	重,有利于缅甸内特任能和女王性
」の 数据接入管理						
↓ Logstash 管理		支持搜索采集器ID / 采集器名称 / ES集群ID / Logs	stash实例ID / CKafka实例ID / Serverless 索引名称	Q	¢	
Beats 管理		平田第10/22 ± 172 平田第35	用 ¥ 卒集関本道 ¥	安備開始出 西木	创建/查测时间	調作
		TORNER TO TORNER	an i ressanceañ l	reconciliante al anti-	E2KE/3C3C3C42140	60% E #*

- 2. 在创建 Metricbeat 采集器中,设置采集器信息。
- 配置 Metricbeat 采集器,输入或选择采集器配置信息。完成后单击下一步。
 - 采集器名称:自定义采集器的名称,格式为1个 50个英文、汉字、数字或下划线(_)。
 - 安装版本: 支持6.8.15、7.10.2或7.14.2版本。
 - 采集器输出:采集的数据支持传送到腾讯云 Elasticsearch 与 Logstash 实例,请选择与需采集数据的 CVM 在同一 VPC 下的 ES 集群和 Logstash 实例。不支持输出至开源版 ES 集群。
 - 用户名密码:若选择输出采集数据到开启用户登录认证的 ES 集群,需要填写用户名和密码,使 Metricbeat 有权限向 ES 集群中写入数据。用户名默认 为 elastic,密码为集群创建时设置。
 - Monitoring: 勾选后在 Kibana 内生成监控 Metricbeat 的相关指标。当采集器输出为 ES 集群时, Monitoring 默认使用和采集器输出相同的 ES 集群;当采集器输出为 Logstash 实例时,则需要在配置文件中额外添加用于存储监控数据的 ES 集群地址。
 - Kibana Dashboard:勾选后生成默认的 Kibana Dashboard。
 - 采集器 YML 配置:

Metricbeat 默认采集系统的监控数据,无需额外配置,如果需要配置采集某项服务例如 Nginx 的监控,可参考官方文档 Configure Metricbeat。



采集器名称 安装版本 *	×	区南头4.50 /D士は樂幸		
安装版本 *		长度万1-50,1X文诗数子。	≥母、汉字、-、下划线	
		请选择	•	
		安装版本需要和采集器输出的	大版本相同	
采集器輸出	*	elasticsearch 💌	· 请选择 ▼ 🗘 新建ES	集群 🖸
		不支持输出到开源版ES集群		
用户名密码:	*	elastic	请填写密码	
启用 Monito	pring			
	-			
官用 Kibana	a Dashboard			
启用 Kibana 采集器YML	a Dashboard 配置			
启用 Kibana 采集器YML metricbe	a Dashboard 配置 eat.yml			
启用 Kibana 采集器YML metricbe	a Dashboard 配置 eat.yml		dules configuration ====================================	
自用 Kibana 采集器YMLI metricbe 1 2	a Dashboard 配置 eat.yml # =======	M	dules configuration	
启用 Kibana 采集器YMLI metricbe 1 2 3	a Dashboard 配置 eat.yml # ================================	.config.modules:	dules configuration ====================================	
启用 Kibana 采集器YML metricbe 1 2 3 4	a Dashboard 配置 eat.yml # ====================================	.config.modules: attern for configurat	dules configuration ====================================	
启用 Kibana 采集器YMLI metricbe 1 2 3 4 5 5	a Dashboard 配置 eat.yml # ====================================	.config.modules: attern for configurat path.config}/modules.	dules configuration ====================================	
启用 Kibana 采集器YMLI 加 1 2 3 4 5 6 7	a Dashboard 配置 eat.yml # ====================================	.config.modules: attern for configurat path.config}/modules.	dules configuration on loading /*.yml	
启用 Kibana 采集器YMLI 1 2 3 4 5 6 7 。	a Dashboard 配置 # ====================================	.config.modules: attern for configurat path.config}/modules. true to enable confi	dules configuration on loading /*.yml reloading	
宮用 Kibana 采集器YMLI metricbe 1 2 3 4 5 6 7 8 8 0	a Dashboard 配置 eat.yml #	.config.modules: attern for configurat path.config}/modules. true to enable confi nabled: false	dules configuration on loading /*.yml reloading	
宮用 Kibana 采集器YMLI 1 2 3 4 5 6 7 8 9 10	a Dashboard 配置 eat.yml # ====================================	.config.modules: attern for configurat path.config}/modules. true to enable confi nabled: false on which files under	dules configuration on loading /*.yml reloading path should be checked for changes	

将采集器安装到 CVM 实例。选择要安装采集器的 CVM 实例,完成后单击确定启用。

○ CVM 必须安装自动化助手,仅支持为已安装自动化助手的 CVM 实例下发采集器配置。



○ 仅支持选择和采集器输出在同一 VPC 下的 CVM 实例进行安装,若无法找到目标 CVM 实例,需要更改采集器输出。

在专有网络 🚯					
安装采集器CVM实例 *					
支持搜索CVM实例ID / 实例名	3称 / 实例标签				Q Ø
CVM实例ID/名称		IP地址	操作系统 🛈	采集器状态	自动化助手 🛈
		公网: 内网:	TencentO	未安装	已安装
		公网: 内网:	TencentO	未安装	已安装
		公网: 内网:	TencentO	未安装	已安装
		公网: 内网:	TencentO	未安装	已安装
	а	公网: 内网:	TencentO	未安装	已安装
		公网: 内网:	TencentO	未安装	已安装
	а	公网: 内网:	TencentO	未安装	已安装
	а	公网: 内网:	TencentO	未安装	已安装
		公网: 内网:	TencentO	未安装	已安装
		公网: 内网:	TencentO	未安装	已安装
共 43 条			10 ▼ 条/页 🛛 🗸	1	/5页 ▶ №

3. 单击确定启用后,跳转到 Beats 采集器管理界面,可以查看 Metricbeat 采集器运行状态,显示"正常"则表示采集器安装成功。支持修改采集器配置和管理 CVM 实例。



Elasticsearch Service	Beats 管理	⑤ 广州 12 平				使月
吉 概览		 对于CVM实例,当前只支持采集Linux系统, 	且CVM实例必须配置腾讯云自动化助手环境。重	看配置指南に		
Serverless 模式						
👶 日志分析		创建采集器				
② 实时搜索						
PaaS 模式		Filebeat	Metricbeat	Auditbeat	Heartbeat	Packetbeat
─ ES 集群管理		轻量的日志采集器,用于收集和传达日 志文件	轻量型指标采集器,用于从系统和服务 收集指标	轻量型审计日志采集器,用于收集 Linux 审计框架的数据	面向运行状态监测的轻量型采集器,通 过主动探测来监测服务的可用性	轻量型网络数据采集器,监测网络流 量,有助于提高网络性能和安全性
℃。ES 索引管理						
@1 数据接入管理			· · · · · · · · · · · · · · · · · · ·			
┃ _■ Logstash 管理		支持搜索采集器ID / 采集器名称 / ES集群ID / Logst	ash实例ID / CKafka实例ID / Serverless 索引名称	Q Ø		
Beats 管理		采集器ID/名称 🕈 状态 采集器类型	』▼ 采集器来源 ▼	采集器输出版本	创建/变更时间	操作
		正常 ⓒ Metr	CVM 正常0/共1台	7.10.2	2023-06-19 17:36:36 2023-06-19 17:37:01	查看全部CVM实例 编辑采集器配置 更多 ▼
		正常 🖹 Fileb	eat TKE		2023-03-07 10:20:41 2023-03-07 10:20:48	编辑采集器配置 更多 ▼

Kibana 查看结果

- 1. 登录腾讯云 Kibana 控制台。
- 2. 在 Kibana 左侧导航栏单击 Discover, 查询 Metricbeat 采集的数据。





创建 Auditbeat 采集审计数据

最近更新时间: 2024-10-12 21:50:12

Auditbeat 是轻量的审计数据采集器,能够收集和监控腾讯云 CVM Linux 审计框架数据,并基于 Kibana 实现可视化分析。

应用场景

Auditbeat 可用于审核 Linux 系统上用户和进程的活动,例如,可以使用 AuditBeat 从 Linux Audit Framework 采集并集中审核事件,也可以使用 Auditbeat 来检测对二进制文件或者配置文件的修改,并发现潜在的安全策略冲突。

Auditbeat 目前有两种模块:

- auditd: auditd 模块用于接收来自 Linux 审计框架的审计事件。审计框架是 Linux 内核的一部分,该模块建立对内核事件的订阅,使得在事件发生时可以 接收到通知。如果使用 auditd 模块,部分系统中其他的监控工具可能会干扰 Auditbeat,例如,在服务器中启用 audit 进程来从 Linux 审计框架中接收数 据,此时 Auditbeat 的运行会收到影响,需要先通过执行 service auditd stop 命令来关闭 auditd 进程。关于该模块更详细的介绍请参考官方文档 Auditd Module。
- file_integrity: file_integrity 模块用于实时监控指定目录下的文件的改动。在 Linux 系统中,需要使用 inofity 才可以启用该模块,2.6.13版本以上的 Linux 内核均已默认安装了 inofity。关于该模块更详细的介绍请参考官方文档 File Integrity Module。

操作须知

∧ 注意

1. 腾讯云 CVM 实例、腾讯云 ES 集群和 Logstash 实例,必须在同一 VPC 下。且腾讯云 ES 集群和 Logstash 实例的大版本相同。

Beats 目前仅支持64位的 Linux 操作系统。

2. 腾讯云 CVM 实例必须安装自动化助手,仅支持为已安装自动化助手的 CVM 实例下发采集器配置。具体操作参见 安装自动化助手客户端 。

操作步骤

Auditbeat 采集器配置

1. 登录 Elasticsearch Service 控制台 Beats 管理界面,授权服务相关角色,单击创建 Auditbeat 采集器。

Elasticsearch Service	Beats 管理 💲 广	H 12 *				
₩b ■ ■ 概 览		对于CVM实例,当前只支持采集Linux系统	,且CVM实例必须配置腾讯云自动化助手环境。 <u>重</u>	香記重 指南 ひ		
Serverless 模式						
昆 日志分析						
② 实时搜索		辺建木果 奋			7	
PaaS 模式 ☴ FS 佳群等理		Filebeat 轻量的日志采集器,用于收集和传达日	 Metricbeat 轻量型指标采集器,用于从系统和服务 	Auditbeat 经量型审计日志采集器。用于收集	Heartbeat 面向运行状态监测的轻量型采集器,通	Packetbeat 经量型网络数据采集器、监测网络流
2 ES 索引管理		志文件	收集指标	Linux 审计框架的数据	过主动探测来监测服务的可用性	量,有助于提高网络性能和安全性
27 数据接入管理					-	
∎ Logstash 管理		支持搜索采集器ID / 采集器名称 / ES集群ID / Logs	tash实例ID / CKafka实例ID / Serverless 索引名称	Q	φ	
Beats 管理		采集器iD/名称 🕈 状态 采集器类	型 Y 采集器来源 Y	采集器输出 版本	创建/变更时间	操作

- 2. 在创建 Auditbeat 采集器中,设置采集器信息。
- 配置 Auditbeat 采集器,输入或选择采集器配置信息。完成后单击下一步。
 - 采集器名称:自定义采集器的名称,格式为1个 50个英文、汉字、数字或下划线(_)。
 - 安装版本: 支持6.8.15、7.10.2或7.14.2版本。
 - 采集器输出:采集的数据支持传送到腾讯云 Elasticsearch 与 Logstash 实例,请选择与需采集数据的 CVM 在同一 VPC 下的 ES 集群和 Logstash 实例。不支持输出至开源版 ES 集群。
 - 用户名密码:若选择输出采集数据到开启用户登录认证的 ES 集群,需要填写用户名和密码,使 Auditbeat 有权限向 ES 集群中写入数据。用户名默认 为 elastic,密码为集群创建时设置。
 - Monitoring:勾选后在 Kibana 内生成监控 Auditbeat 的相关指标。当采集器输出为 ES 集群时,Monitoring 默认使用和采集器输出相同的 ES 集群;当采集器输出为 Logstash 实例时,则需要在配置文件中额外添加用于存储监控数据的 ES 集群地址。
 - Kibana Dashboard:勾选后生成默认的 Kibana Dashboard。
 - 采集器 YML 配置: auditd 模块和 file_integrity 模块配置如下,更多 YML 配置请参考官方文档 Configure modules。
 - auditd 模块:



- audit_rule_files:指定的审计规则文件路径,支持通配符。
- audit_rules: 自定义的审计规则(一般情况下默认的审计规则就可以满足审计需求)。
- file_integrity 模块:
 - paths:用于指定被监控的文件的路径,默认的文件路径包含 /bin、/usr/bin、/sbin、/usr/sbin、/etc。

	uditbeat采集器 > 2 将采集器安装到CVM实例	
采集器名称	test	
安装版本 *	7.10.2 *	
	安装版本需要和采集器输出的大版本相同	
采集器输出	elasticsearch 🔹 🗘 新建ES集群 🖸	
	不支持輸出到开源版ES集群	
用户名密码	elastic 请填写密码	
启用 Monito		
启用 Kibana	ashboard Q 只有ES实例和采集器的前两位版本号相同才能开启dashboard	
采集器YML		
auditbea	ymi	
1	Modules configuration	
1 2 3	<pre></pre>	
1 2 3 4	<pre>module: auditd</pre>	
1 2 3 4 5	<pre>module: auditd # Load audit rules from separate files. Same format as audit.rules(7).</pre>	
1 2 3 4 5 6	<pre>module: auditd # Load audit rules from separate files. Same format as audit.rules(7). audit_rule_files: ['\${path.config}/audit.rules.d/*.conf']</pre>	
1 2 3 4 5 6 7	<pre>modules configuration ====================================</pre>	
1 2 3 4 5 6 7 8	<pre>modules configuration ====================================</pre>	
1 2 3 4 5 6 7 8 9	<pre>modules configuration wditbeat.modules: module: auditd # Load audit rules from separate files. Same format as audit.rules(7). audit_rule_files: ['\${path.config}/audit.rules.d/*.conf'] audit_rules: ## Define audit rules here. ## Create file watches (-w) or syscall audits (-a or -A). Uncomment these</pre>	
1 2 3 4 5 6 7 8 9 10	<pre>module: auditd # Load audit rules from separate files. Same format as audit.rules(7). audit_rule_files: ['\${path.config}/audit.rules.d/*.conf'] audit_rules: ## Define audit rules here. ## Create file watches (-w) or syscall audits (-a or -A). Uncomment these ## examples or add your own rules.</pre>	

- 将采集器安装到 CVM 实例。选择要安装采集器的 CVM 实例,完成后单击确定启用。
 - CVM 必须安装自动化助手,仅支持为已安装自动化助手的 CVM 实例下发采集器配置。



○ 仅支持选择和采集器输出在同一 VPC 下的 CVM 实例进行安装,若无法找到目标 CVM 实例,需要更改采集器输出。

专有网络 🛈				
₩装采集器CVM实例 *				
持搜索CVM实例ID / 实例名称 / 》	实例标签			Q Ø
CVM实例ID/名称	IP地址	操作系统 🛈	采集器状态	自动化助手 🕄
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
43 옾		10 ▼ 条/页 🛛 🛛	1	/5页 🕨 🕨

3. 单击确定启用后,跳转到 Beats 采集器管理界面,可以查看 Auditbeat 采集器运行状态,显示"正常"则表示采集器安装成功。支持修改采集器配置和管理 CVM 实例。

Kibana 查看结果



1. 在 Kibana 左侧导航栏单击 Discover, 查询 Auditbeat 采集的数据:

Discover															New	Save	Open	Share	Inspect
🗒 🗸 Search									ĸ	QL 🛗) ~	Last 15 minut	es			Sho	ow dates	G	Refresh
🖘 – + Add filter																			
auditbeat-* \checkmark	€		3,536 hits																
Q Search field names							Sep 2	7, 2021 @	17:14:39.0	79 - Sep	27, 20	21 @ 17:29:39	9.079 A	uto	\sim				
🗟 Filter by type	0		2000																
Selected fields			1500																
(_source		ount	1000											_					
Available fields		0	500																
t_id																			
t _index			0	17:15:00	17:16:00	17:17:00	17:18:00	17:19:00	17:20:00	17:21:00	17:22:	00 17:23:00	17:24:00	17:25:00	17:26:00	17:27:00	17:28:00	17:29:00	
# _score										@time	estamp	per 30 second	s						
t _type			Time 🖵			_sc	ource												
📋 @timestamp		~ .	Son 27	2021 @	17.20.20	250													
t agent.ephemeral_id			Jep 27	, 2021 @	17.29.30	.000 @t	:imestamp:	Sep 27,	2021 @ 1/	:29:30.3	ser sver b	vtes: 348 r	receiver	.barad.mo	nitor.te	ncentcs.co	related	.1p: 169	.254.0.4
t agent.hostname						hc	st.os.fam	ily: redh	at host.	os.name:	Cent08	S Linux host	.os.kerne	el: 3.10.	0-693.el	7.x86_64	host.os.co	odename:	Core

2. 在 Kibana 左侧导航栏,单击 Dashboard,在 Dashboard 列表中,单击 [Auditbeat File Integrity] Overview,查看监控文件的变动情况:





创建 Heartbeat 采集服务器状态

最近更新时间: 2024-10-12 21:50:12

Heartbeat 是轻量的运行状态监测数据采集器,支持 ICMP 监视(包括 ICMPV4 和 ICMPV6)、TCP 监视和 HTTP 监视,能够主动探测服务的可用性。

应用场景

Hearbeat 通过主动探测来检测服务的可用性,可以通过给定 URL 列表对网站运行状况进行监控,支持通过 ICMP、TCP、HTTP 进行 ping 检测,同时也支 持 TLS、身份验证和代理。Heartbeat 通过配置 monitors 进行检测指定主机或者网站的运行情况,目前支持三种 monitor:

- ICMP: 支持 IPV4 和 IPV6,发送 ICMP 请求检测服务是否可用,该 monitor 需要 root 权限。
- TCP:发送 TCP 请求检测服务是否可用。
- HTTP:发送 HTTP 请求检测服务是否可以正常响应,以及响应状态码、响应头部或者内容是否正确。

操作须知

1. 腾讯云 CVM 实例、腾讯云 ES 集群和 Logstash 实例,必须在同一 VPC 下。且腾讯云 ES 集群和 Logstash 实例的大版本相同。

≙	注意
	Beats 目前仅支持64位的 Linux 操作系统。

2. 腾讯云 CVM 实例必须安装自动化助手,仅支持为已安装自动化助手的 CVM 实例下发采集器配置。具体操作参见 安装自动化助手客户端 。

操作步骤

Heartbeat 采集器配置

1. 登录 Elasticsearch Service 控制台 Beats 管理界面,授权服务相关角色,单击创建 Heartbeat 采集器。

Beats 管理 💿 广州(3) • 🗸				Beats使用指南 已
i 当前只支持下发Beats至Linux 64位系	统的CVM实例,且CVM实例必须配置腾讯云目	自动化助手环境。Beats不支持输出至开源版6	Elasticsearch集群,查看配置指南 🖸	
创建采集器 Filebeat 轻量的日志采集器,用于 收集和传达日志文件	 	Ling Auditbeat 轻量型审计日志采集器, 用于收集 Linux 审计框架 的数据	Heartbeat 面向运行状态监测的轻量 型采集器,通过主动探测 来监测服务的可用性	Packetbeat 轻量型网络数据采集器, 监测网络流量,有助于提 高网络性能和安全性

2. 在创建 Heartbeat 采集器中,设置采集器信息。

- 配置 Heartbeat 采集器,输入或选择采集器配置信息。完成后单击下一步。
 - 采集器名称:自定义采集器的名称,格式为1个 50个英文、汉字、数字或下划线(_)。
 - 安装版本: 支持6.8.15、7.10.2或7.14.2版本。
 - 采集器输出:采集的数据支持传送到腾讯云 Elasticsearch 与 Logstash 实例,请选择与需采集数据的 CVM 在同一 VPC 下的 ES 集群和 Logstash 实例。不支持输出至开源版 ES 集群。
 - 用户名密码:若选择输出采集数据到开启用户登录认证的 ES 集群,需要填写用户名和密码,使 Heartbeat 有权限向 ES 集群中写入数据。用户名默认 为 elastic,密码为集群创建时设置。
 - Monitoring:勾选后在 Kibana 内生成监控 Heartbeat 的相关指标。当采集器输出为 ES 集群时,Monitoring 默认使用和采集器输出相同的 ES 集群;当采集器输出为 Logstash 实例时,则需要在配置文件中额外添加用于存储监控数据的 ES 集群地址。
 - Kibana Dashboard:勾选后生成默认的 Kibana Dashboard。
 - 采集器 YML 配置: 配置内容如下, 更多 YML 配置请参考官方文档 Configure Hearbeat。
 - type: monitor 类型,支持 icmp、tcp、http。
 - id: 自定义的 monitor 名称。
 - name: 自定义的 monitor 名称。



- hosts:指定要检测的服务地址。
- schedule: 检测频率, */5 * * * * * * 表示每隔5s检测一次。
- check.response.status:当 monitor为 http 时, http 接口正常响应时的状态码,如200。

1 配	晋Heartbeat采	集器 〉 ② 約	8采集器安装到CVM实例	
《集器名利	称 *	长度为1-50,仅支持数字	、字母、汉字、-、下划线	
、 装版本 •	*	请选择	•	
		安装版本需要和采集器输出	的大版本相同	
《集器输出	出*	elasticsearch	▼ 请选择 ▼	
		不支持輸出到开源版ES集翻	Ť	
月户名密码	码 *	elastic	请填写密码	
月户名密码 引用 Moni	码 * itoring	elastic	请填写密码	
引户名密码 引用 Moni 引用 Kibai	태oring ana Dashboard	elastic	请填写密码	
月戸名密研 日用 Moni 日用 Kibai ミ集器YM	码 * hitoring ana Dashboard AL配置	elastic	请填写密码	
目户名密码 目用 Moni 目用 Kibai 総集器YM heartb	码 * hitoring ana Dashboard AL配置 Deat.yml	elastic	请填写密码	
目户名密码 引用 Moni 引用 Kibai 候集器YM heartb 1	码 * hitoring ana Dashboard //L配置 Deat.yml	elastic	请填写密码	
引户名密码 引用 Moni 引用 Kibai 後集器YM heartb 1 2	码 * hitoring ana Dashboard //L配置 peat.yml ###############################	elastic	请填写密码 Heartbeat ####################################	
引户名密码 引用 Moni 引用 Kibai 条集器YM heartb 1 2 3	码 * hitoring ana Dashboard AL配置 peat.yml ####################################	elastic	请填写密码 Heartbeat ####################################	
引户名密码 引用 Moni 引用 Kibal 集器YM heartb 1 2 3 4 5	码 * Nitoring ana Dashboard AL配置 Deat.yml ########## # Define a # of indiv	elastic	请填写密码 Heartbeat ####################################	
l户名密码 l用 Moni l用 Kibai k集器YM heartb 1 2 3 4 5 6	码 * Witoring ana Dashboard AL配置 Deat.yml ########## # Define a # of indiv beartheat	elastic	请填写密码 Heartbeat ####################################	
l户名密码 l用 Moni l用 Kibai 条集器YM heartb 1 2 3 4 5 6 7	码 * Witoring ana Dashboard AL配置 beat.yml ########## # Define a # of indiv heartbeat. # Direct	elastic	请填写密码 Heartbeat ####################################	
l户名密码 l用 Moni l用 Kibai 条集器YM heartb 1 2 3 4 5 6 7 8	码 * hitoring ana Dashboard AL配置 beat.yml ########## # Define a # of indiv heartbeat. # Direct path: \${	elastic	请填写密码 Heartbeat ####################################	
l户名密码 l用 Moni l用 Kibai 条集器YM heartb 1 2 3 4 5 6 7 8 9	码 * hitoring ana Dashboard AL配置 beat.yml ########## # Define a # of indiv heartbeat. # Direct path: \${ # If ena	elastic	请填写密码 Heartbeat ####################################	inges
引户名密码 引用 Moni 引用 Kibai 後集器YM heartb 1 2 3 4 5 6 7 8 9 10	码 * hitoring ana Dashboard AL配置 Deat.yml ########## # Define a # of indiv heartbeat. # Direct path: \${ # If ena reload.e	<pre>elastic ###################################</pre>	请填写密码 Heartbeat ####################################	inges

- 将采集器安装到 CVM 实例。选择要安装采集器的 CVM 实例,完成后单击确定启用。
 - CVM 必须安装自动化助手,仅支持为已安装自动化助手的 CVM 实例下发采集器配置。



○ 仅支持选择和采集器输出在同一 VPC 下的 CVM 实例进行安装,若无法找到目标 CVM 实例,需要更改采集器输出。

在专有网络 🛈				
安装采集器CVM实例 *				
支持搜索CVM实例ID / 实例名称 / §	2.例标签			Q Ø
CVM实例ID/名称	IP地址	操作系统 🛈	采集器状态	自动化助手 🛈
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
共 43 条		10 ▼ 条/页 🛛 🗸	(1	/5页 ▶ ▶

3. 单击确定启用后,跳转到 Beats 采集器管理界面,可以查看 Heartbeat 采集器运行状态,显示"正常"则表示采集器安装成功。支持修改采集器配置和管理 CVM 实例。

Kibana 查看结果

1. 登录腾讯云 Kibana 控制台。



2. 在 Kibana 左侧导航栏单击 Discover, 查询 Heartbeat 采集的数据。

Search											KQL	•	Last 1 hour		Show da	tes C Refres
🗇 – + Add filter																
heartbeat-* \checkmark		€							:	20 hits						
Q Search field names								Sep 28, 2021 @ 1	4:59:05.051 - Sep :	28, 2021 @ 15:59:05.05	i1 Auto	~				
Filter by type	0		6													
Selected fields			5													
(0) _source			3 ount													
Available fields			2													
t_id			1													
t_index			0	15:00	15:05	15:10	15:15	15:20	15:25	15:30	15:35		15:40	15:45	15:50	15:55
/ _score									@tim	estamp per minute						
t_type			Tim	e 🗸		_source										
🔲 @timestamp			> Sep	28. 2021 @ 15:	8:54.788	Stimostoma: Son 28	0001 @ 15-50-54 3	198 top stt oppoor	t up: 1 207 http		401					
t agent.ephemeral_id				20, 2021 0 1010		http.response.body.h	ash: 961eeb737caf	1c461169576885b3e8	1,207 http: 15340e4222f167b09e	0f438f0e95704a084 ht	tp.respor	nse . hodv .	bytes: 381 htt	n response body c	ontent: {"error":{"ro	ot cause":
t agent.hostname						[{"type":"security_ex	ception","reason	":"missing authenti	ication credential	ls for REST request [/]", "head	ler":{"WW	W-Authenticate"	:"Basic realm=\"s	ecurity\" charset=\"U	re-
t agent.id						8\""}}],"type":"secur	ity_exception","	reason":"missing au	uthentication cred	dentials for REST req	uest [/]"	, "header	":{"WWW-Authent	icate":"Basic rea	lm=\"security\" chars	et=\"UTF-



创建 Packetbeat 采集网络流量

最近更新时间: 2024-10-12 21:50:12

Packetbeat 是轻量的网络流量包采集器,用于应用程序和性能监测,支持将数据传输至 logstash 实例或 Elaticsearch 集群中进行分析,并在 Kibana 中 可视化查看。

应用场景

Packetbeat 通过采集应用层的网络流量数据(HTTP、MySQL、Redis 等),使得用户可以密切监测应用程序的延迟和错误、响应时间、SLA 性能、用户 访问模式和趋势等。

操作须知

• 腾讯云 CVM 实例、腾讯云 ES 集群和 Logstash 实例,必须在同一 VPC 下。且腾讯云 ES 集群和 Logstash 实例的大版本相同。



• 腾讯云 CVM 实例必须安装自动化助手,仅支持为已安装自动化助手的 CVM 实例下发采集器配置。具体操作参见 安装自动化助手客户端。

操作步骤

Packetbeat 采集器配置

1. 登录 Elasticsearch Service 控制台 Beats 管理界面,并授权服务相关角色,单击创建 Packetbeat 采集器。

唐讯云 ∩ 总第	□ 云产品 ~				搜索产品、文档 Q, 🕜 小程序	☑ 集团账号◇ 备案 工具◇ 客	服支持~ 费用 ~ 🛛 🥆
Elasticsearch Service	Beats 管理 💲 广,	∜12 ▼					使用指南 🖸
器 概 览		⑦ 对于CVM实例,当前只支持采集Linux系统,	且CVM实例必须配置腾讯云自动化助手环境。重要	配置指南 亿			
Serverless 模式							
誌 日志分析							
② 实时搜索		初建米興谷					1
PaaS 模式		Filebeat	Metricbeat	Auditbeat	Weartbeat	Packetbeat	
─ ES 集群管理		轻量的日志采集器,用于收集和传达日 志文件	轻量型指标采集器,用于从系统和服务 收集指标	轻量型审计日志采集器,用于收集 Linux 审计框架的数据	面向运行状态监测的轻量型采集器,通 过主动探测来监测服务的可用性	轻量型网络数据采集器,监测网络流 量、有助于提高网络性能和安全性	
℃。ES 索引管理							
@ 数据接入管理							1
┃。 Logstash 管理		支持搜索采集器ID / 采集器名称 / ES集群ID / Logsta	sh实例ID / CKafka实例ID / Serverless 索引名称	Q	¢		
Beats 管理		采集器ID/名称 本 状态 采集器类型	▼ 采集器来源 ▼	采集器输出 版本	创建/变更时间	操作	
						the set of the set of the set	

- 2. 在创建 Packetbeat 采集器中,设置采集器信息。
- 配置 Packetbeat 采集器,输入或选择采集器配置信息。完成后单击下一步。
 - 采集器名称:自定义采集器的名称,格式为1个 50个英文、汉字、数字或下划线(_)。
 - 安装版本: 支持6.8.15、7.10.2或7.14.2版本。
 - 采集器输出:采集的数据支持传送到腾讯云 Elasticsearch 与 Logstash 实例,请选择与需采集数据的 CVM 在同一 VPC 下的 ES 集群和 Logstash 实例。不支持输出至开源版 ES 集群。
 - 用户名密码:若选择输出采集数据到开启用户登录认证的 ES 集群,需要填写用户名和密码,使 Packetbeat 有权限向 ES 集群中写入数据。用户名默 认为 elastic,密码为集群创建时设置。
 - Monitoring:勾选后在 Kibana 内生成监控 Packetbeat 的相关指标。当采集器输出为 ES 集群时,Monitoring 默认使用和采集器输出相同的 ES 集群;当采集器输出为 Logstash 实例时,则需要在配置文件中额外添加用于存储监控数据的 ES 集群地址。
 - Kibana Dashboard:勾选后生成默认的 Kibana Dashboard。
 - 采集器 YML 配置: Packetbeat 支持采集多种协议的网络流量,具体每个协议的参数可参考官方文档 Configure Packetbeat。



	称*	长度为1-50,仅支持数号	又字、-、下划线	
安装版本	*	请选择	v	
			目同	
《集器输	出*	elasticsearch	选择 ▼ ∲ 新建ES集 群	ß
1月 二 名密	码 *	elastic	直写密码	
⊇⊞ Mon	aitorina			
当用 Mon	nitoring			
自用 Mon 自用 Kiba	nitoring ana Dashboar			
∃用 Mon ∃用 Kiba ≤年器VM	nitoring ana Dashboar vu 하응	d O		
目用 Mon 目用 Kiba 彩集器YN packe	nitoring ana Dashboar ML配置 atheat yml	d O		
目用 Mon 日用 Kiba 彩集器YN packe	nitoring ana Dashboar ML配置 e tbeat.yml	d		
目用 Mon 日用 Kiba K集器YN packe 1	nitoring ana Dashboar ML配置 etbeat.yml # ======	d O	work device ====================================	
引用 Mon 引用 Kiba 終集器YN packe 1 2	nitoring ana Dashboar WL配登 etbeat.yml # ====== # Coloria		work device	
計 Mon 計 Kiba 後集器YN packe 1 2 3 4	nitoring ana Dashboar WL配置 etbeat.yml # ====== # Select # "apy."	t the network interfac	work device	
引用 Mon 引用 Kiba 使集器YN packe 1 2 3 4 5	nitoring ana Dashboar WL配置 etbeat.yml # ====== # Select # "any" packeth	t the network interfac keyword to sniff on a	work device Iff the data. On Linux, you can use the ected interfaces.	
明 Mon 訳用 Kiba 集器YN packe 1 2 3 4 5 6	nitoring ana Dashboar WL配置 #tbeat.yml # ====== # Select # "any" packetbo	t the network interface keyword to sniff on a eat.interfaces.device:	work device ====================================	
目用 Mon 日用 Kiba 条集器YN packe 1 2 3 4 5 6 7	nitoring ana Dashboar WL配置 etbeat.yml # select # "any" packetbe # =====	t the network interfac keyword to sniff on a eat.interfaces.device:	work device ====================================	==
目用 Mon 日用 Kiba 采集器YN packe 1 2 3 4 5 6 7 8	nitoring ana Dashboar WL配置 etbeat.yml # select # "any" packetbe # ======	t the network interface keyword to sniff on a eat.interfaces.device:	work device Iff the data. On Linux, you can use the ected interfaces. Flows	==
引用 Mon 引用 Kiba 条集器YN packe 1 2 3 4 5 6 7 8 9	nitoring ana Dashboar WL配置 # etbeat.yml # Select # "any" packetbo # ====== # Set er	t the network interface keyword to sniff on a eat.interfaces.device:	work device Iff the data. On Linux, you can use the ected interfaces. Flows	==
目用 Mon 日用 Kiba 条集器YN packe 1 2 3 4 5 6 7 8 9 10	nitoring ana Dashboar WL配置 # setbeat.yml # setect # "any" packetbo # ====== # Set er packetbo	t the network interfac keyword to sniff on a eat.interfaces.device:	work device Iff the data. On Linux, you can use the ected interfaces. Flows all options to disable flows reporting.	==

• 将采集器安装到 CVM 实例。选择要安装采集器的 CVM 实例,完成后单击确定启用。

○ CVM 必须安装自动化助手,仅支持为已安装自动化助手的 CVM 实例下发采集器配置。



○ 仅支持选择和采集器输出在同一 VPC 下的 CVM 实例进行安装,若无法找到目标 CVM 实例,需要更改采集器输出。

✔ 配置Packetbeat采集器 〉	2 将采集器安装到CVM实例			
在专有网络 🛈				
F安装采集器CVM实例★				
支持搜索CVM实例ID / 实例名称 / 实例标签				Q Ø
CVM实例ID/名称	IP地址	操作系统 🛈	采集器状态	自动化助手 🛈
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
	公网: 内网:	TencentO	未安装	已安装
共 43 条	10 💌	条/页 ▮ ◀	1	/5页 ▶ ▶

3. 单击确定启用后,跳转到 Beats 采集器管理界面,可以查看 Packetbeat 采集器运行状态,显示"正常"则表示采集器安装成功。支持修改采集器配置和管理 CVM 实例。

Kibana 查看结果

1. 登录腾讯云 Kibana 控制台。



腾讯云

2. 在 Kibana 左侧导航栏单击 Discover, 查询 Packetbeat 采集的数据:





管理 CVM 实例

最近更新时间: 2024-10-12 21:50:12

完成采集器安装后,可通过 Beats 管理功能,查看和管理采集器下发的全部 CVM 实例。

操作步骤

1. 登录 Elasticsearch Service 控制台 Beats 管理,确保已经创建 Beats 采集器。

Beats 管理)广州 12 🔻							Elasticsearch技术社区	Beats使用指南
() 对于CVM实行	列,当前只支持	采集Linux系统,且CVM	实例必须配置腾讯云自动	比助手环境。查看配置指南 🖸					
创建采集器									
Filebe 轻量的日志采集 和传达日志文件	eat ^{集器} ,用于收集 ‡	 ・ ・	tricbeat 采集器,用于从系 集指标	Auditbeat Auditbeat 经量型审计日志采集器,用 收集 Linux 审计框架的数据	Ŧ	 Hearth 面向运行状态监 集器,通过主动 务的可用性 	beat 测的轻量型采 p探测来监测服	⑦ Packetb 轻量型网络数据采 网络流量,有助于 能和安全性	eat 集器,监测 提高网络性
支持搜索采集器ID/3	采集器名称 / Es	G集群ID / Logstash实例II) / CKafka实例ID / Serve	rless 索引名称		Q	φ		
采集器ID/名称 🕈	状态	采集器类型 ▼	采集器来源 ▼	采集器输出	采集器版本		创建/变更时间	操作	
	正常	ilebeat	CVM 正常0/共1台	Elasticsearch集群. es-7ah3kajs	7.14.2		2023-03-23 17:1 2023-03-23 17:1	<u>查看全部C</u> 4:18 编辑采集器 4:42 更多 ▼	VM实例 配置

2. 在采集器列表中,选择**操作 > 查看全部 CVM 实例**,可以管理 Filebeats 采集器下运行的全部 CVM 实例。若 CVM 实例的采集器运行情况显示"心跳正 常",说明采集器在该 CVM 实例上的采集任务正常运行。

采集器全部CVM实例				×
添加CVM实例	支持搜索CVM实例ID / 实例名称	你/实例标签		Q Ø
✓ CVM实例 ID/名称	IP地址	操作系统	采集器运行情况	操作
	公网: 内网:	CentOS 7.5 64bit	⊘ 心跳正常	Ū
共 1 条		5 ▼ 条/页	⊌ ∢ 1	/1页 🕨 🕨
移除CVM实例	取消			



通过 Filebeat 采集 TKE 容器日志

最近更新时间: 2024-10-12 21:50:12

对于需要采集并分析腾讯云 TKE 容器日志的场景,可以使用 Filebeat 采集数据,并将采集的数据传输到腾讯云 Elasticsearch 集群中进行存储,如果需要加 工与处理,也可以先将数据发送到腾讯云 Logstash 中进行过滤与预处理,最终可以在 Kibana 中查询并分析日志。本文介绍如何配置 Filebeat 采集部署在腾 讯云的 TKE 容器日志。

应用场景

Filebeat 是一个轻量型的日志采集器,可以轻松地采集云上的 TKE 容器日志,从而使得查询或者分析业务服务端的日志变得简单。

- Filebeat 能够逐行读取并发送日志,支持在出现中断的情况下,记录中断时读取到的文件位置信息,后续恢复正常后可以从中断前停止的位置继续开始。
- Filebeat 非常适合采集 nginx、apache 以及容器服务的日志,并且提供可以直接引用的配置模板,极大的简化了这类服务的日志采集过程。

操作须知

- 腾讯云 TKE 实例、腾讯云 ES 集群和 Logstash 实例,必须在同一 VPC 下,且腾讯云 ES 集群和 Logstash 实例的大版本相同。
- TKE集群需要是运行中状态且为标准集群。

操作步骤

Filebeat 采集器配置

1. 登录 Elasticsearch Service 控制台 Beats 管理界面,授权服务相关角色,在 Filebeat 采集器选择 TKE 日志采集。

Beats 管理	⑤ 广州(6) [●] ▼						
	① 对于CVM实例,当前只支持采集Linux系统,且CVM实例必须配置腾讯云自动化助手环境。查看配置指南 I2 创建采集器						
	Filebeat 轻量的日志采集器,用于收集	Metricbeat 经量型指标采集器,用于从系 依如即复步使带地与	Auditbeat 轻量型审计日志采集器,用于	Heartbeat 面向运行状态监测的轻量型采 使習 タンキントが認知せば可容	Packetbeat 经量型网络数据采集器,监测 PACketbeat		
	CVM日志采集 TKE日志采集	幼儿和山政为4次来了目初	收集 Linux 申订性朱的政雄	来奇,迪及土动探测米监测敞 务的可用性	能和安全性		

2. 在创建 Filebeat 采集器中,设置采集器相关信息。

2.1 第一步,选择输出目的:

- 采集器名称:必填。自定义采集器的名称。
- 安装版本:必选。支持6.8.21、7.10.2、7.14.0、7.17.1,安装版本需要和采集器输出的大版本相同。
- 采集器输出:必选。采集的数据支持传送到腾讯云 Elasticsearch 集群与 Logstash 实例,请选择与需采集数据的 TKE 在同一 VPC 下的 ES 集群 和 Logstash 实例。不支持输出至开源版 ES 集群。
- 用户名密码:必填。若选择输出采集数据到开启用户登录认证的 ES 集群,需要填写用户名和密码,使得 Filebeat 有权限向 ES 集群中写入数据。用户 名默认为 elastic,密码为集群创建时设置。
- 启用 Monitoring:可选。勾选后生成监控 Filebeat 的相关指标。当采集器输出为 ES 集群时,Monitoring 默认使用和采集器输出相同的 ES 集群; 当采集器输出为 Logstash 实例时,则需要在配置文件中额外添加用于存储监控数据的 ES 集群地址。
- 启用 Kibana Dashboard:可选。勾选后生成默认的 Kibana Dashboard。



创建Filebeat采集器(采集TKE容器日志)	×
	1 选择输出目的 > 2 配置采集来源	
采集器名称 *	长度为1-50,仅支持数字、字母、汉字、下划线	
安装版本 *	请选择 ▼	
	安装版本需要和采集器输出的大版本相同	
采集器输出 *	elasticsearch す 造 择 ず が 新 建 ES 集 群 ど	
	不支持输出到开源版ES集群	
用户名密码 ★		
启用 Monitoring		
启用 Kibana Dashboard		
	下一步取消	

2.2 第二步,配置采集来源:

- 所在私有网络 VPC: 默认使用上一步采集器输出选择的实例的 VPC, 且不可更改。
- 待采集 TKE 集群 ID:必选。需采集的 TKE 集群的 ID,TKE 集群需要是运行中状态且为标准集群。
- 采集配置:可通过单击添加来横向增加更多采集配置,上限10个。
- 采集配置名称:必填。
- 命名空间:必选。第一个下拉可选择 包含/不包含。第二个下拉可选择命名空间,支持多选,不支持选择不包含全部命名空间。
- Pod 标签:选填。支持创建多个 Pod 标签,标签之间是逻辑与关系。
- 容器名称:选填。填写的容器名称必须在采集目标集群及命名空间之下,为空时,Filebeat 会采集命名空间下符合 Pod 标签的全部容器。
- 写入的索引名称前缀:选填。写入的索引名称前缀将作为 ES 索引名称的一部分,例如替代 filebeat-%{[index]}-%{+yyyy.MM.dd}中的 index 。
- 日志内容过滤:选填。根据关键字过滤日志,可填多个关键字,以逗号分隔。



高级采集配置:选填。个性化设置解析方式	忧、过滤等, <i>一</i> 般采用默认配置,	详情请参见 配置文件填写参考。
---------------------	--------------------------	-----------------

E私有网络VPC					
条集TKE集群ID ⑦★	■选择 ▼				
采集配置 + 添加					
采集配置名称 *	长度为1-30,仅支持数字、字母、下划线				
从哪里采集					
命名空间 *	包含 🔻				
Pod 标签		删除			
	新增				
容器名称	请输入容器名称,留空则采集符合以上Pod 标签的全部容器日志。				
解析和处理					
写入的索引名称前缀 🗿	长度为1-50, 仅支持数字、字母、下划线				
	将作为ES索引名称的一部分				
日志内容过滤	请输入待过滤的关键字,以英文逗号分隔				
高级采集配置	个性化设置解析方式、过滤等,一般采用默认配置。修改 🔻				
2 process 3 - dec 4 f 5 p 6 m 7 t 8 0 9 a 10 - dro 11 f 12 j 13	ors: ode_json_fields: lelds: ["message"] rocess_array: false ix_depth: 1 arget: "" rerwrite_keys: false Id_error_key: true fields: lelds: ["field1", "field2"] gnore_missing: false				
		配置文件填写参考			



3. 单击确定启用后,跳转到 Beats 采集器管理界面,可以查看 Filebeat 采集器运行状态,显示"正常"则表示采集器安装成功。

Beats 管理) 广州 12 👻							Elasticsearch技术社区	Beats使用指南
① 对于CVM实例,当前只支持采集Linux系统,且CVM实例必须配置腾讯云自动化助手环境。查看配置指南 IZ									
创建采集器									
Filebea	at	(Met	ricbeat	Auditbeat		Heart	beat	Packetbe	eat
轻量的日志采集器,用于收集 和传达日志文件		轻量型指标。 统和服务收缩	《集器,用于从系 具指标	轻量型审计日志采集器,用于 收集 Linux 审计框架的数据	用于 面向运行状态监测的轻 据 集器,通过主动探测来 务的可用性		這则的轻量型采 助探测来监测服	轻量型网络数据采集器,监测 网络流量,有助于提高网络性 能和安全性	
支持搜索采集器ID / 采	《集器名称 / ES复	『群ID / Logstash实例ID	/ CKafka实例ID / Serve	rless 索引名称		Q	¢		
采集器ID/名称 ◆	状态	采集器类型 ▼	采集器来源 ▼	采集器输出	采集器版	本	创建/变更时间	操作	
	正常	ilebeat	CVM 正常0/共1台	Elasticsearch集群: es-7ah3kajs	7.14.2		2023-03-23 17:14: 2023-03-23 17:14:	查看全部CV :18 编辑采集器 :42 更多 ▼	/M实例 配置

Logstash 管道配置

腾讯云

如需将采集的日志数据传送到腾讯云 Logstash 实例,可参考 接收 Filebeat 发送的数据并写入到 Elasticsearch 配置 Logstash 管道。

Kibana 查看结果

- 1. 登录腾讯云 Elasticsearch Service 的 Kibana 控制台。
- 2. 左侧导航栏单击 Dev Tool,执行下述语句,查看采集成功的数据。

GET filebeat-7.10.2/_search