Elasticsearch Service

Beats 指南

Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

Contents

Beats 指南

概述

Last updated：2024-03-06 22:05:31

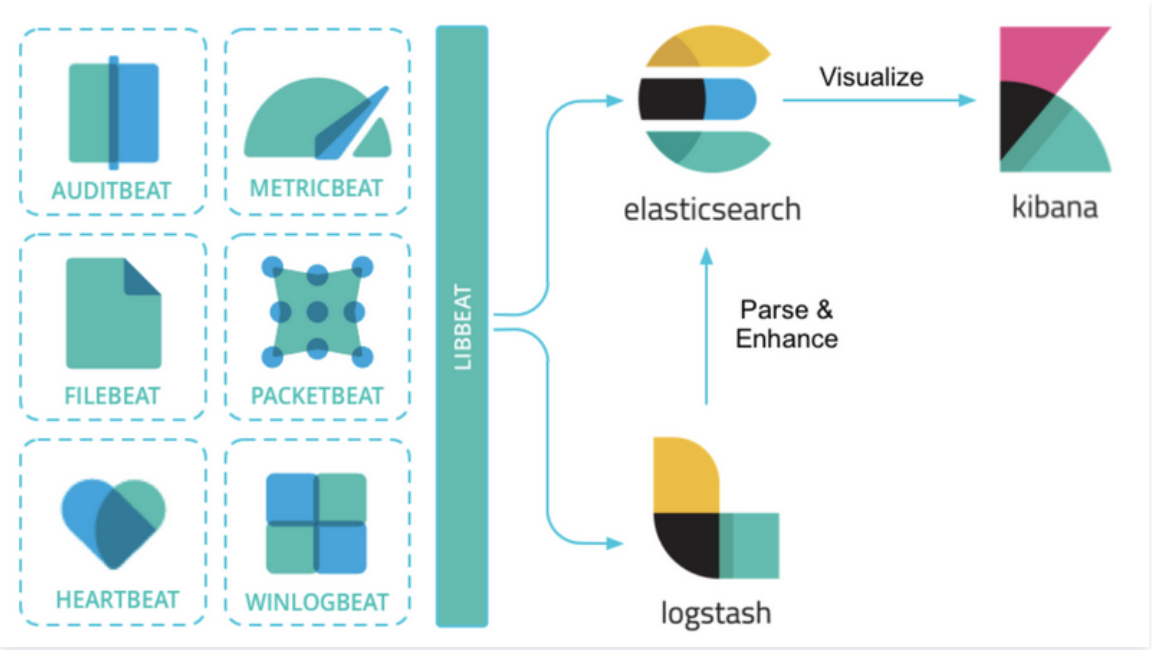
腾讯云 Beats 是基于开源的轻量数据采集器平台 Beats 构建的云端托管服务，提供自动化的 Beats 采集器配置下发服务，支持采集 CVM 服务数据，并发送到腾讯云 ElasticSearch 集群或 Logstash 实例。

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

Last updated：2024-03-06 22:05:31

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

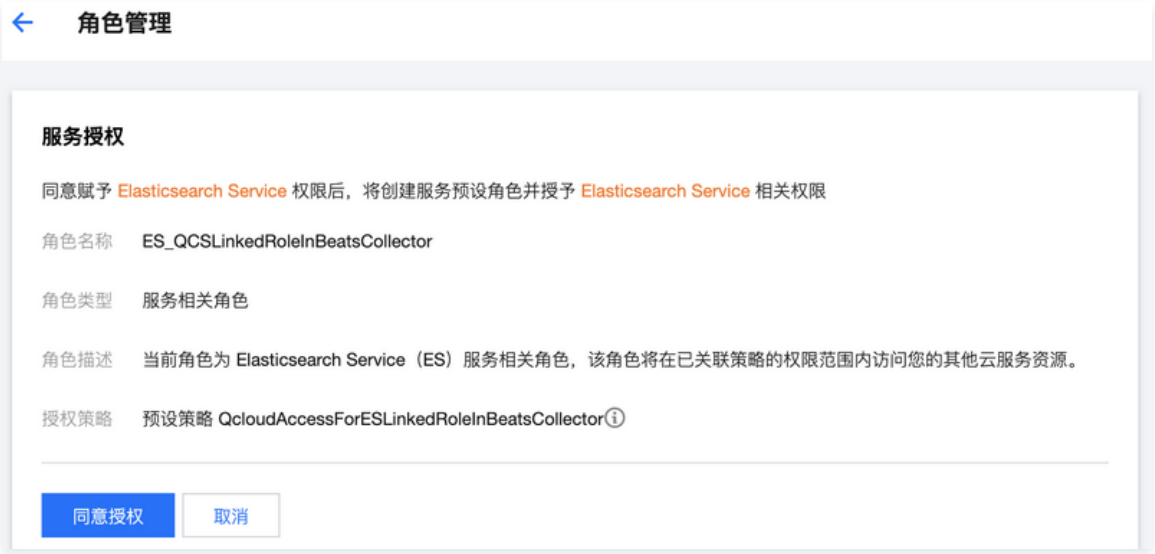
当您已注册并登录腾讯云账号后，首次创建 Beats 服务时，腾讯云 ES 将自动创建具有执行任务权限的角色，并默认出现授权界面，引导您跳转**访问管理**页面，对当前角色授予操作云服务器（CVM）、腾讯云自动化助手（TAT）等其他云资源的权限。腾讯云 ES 通过扮演该角色，即可调用相关 API，完成 Beats 采集器在 CVM 机器上的数据采集任务。

> **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
QcloudAccessForESLinkedRoleInBeatsCollector	该策略仅供腾讯云 Elasticsearch Service（ES）服务相关角色（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

Last updated：2024-10-12 21:50:12

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**。

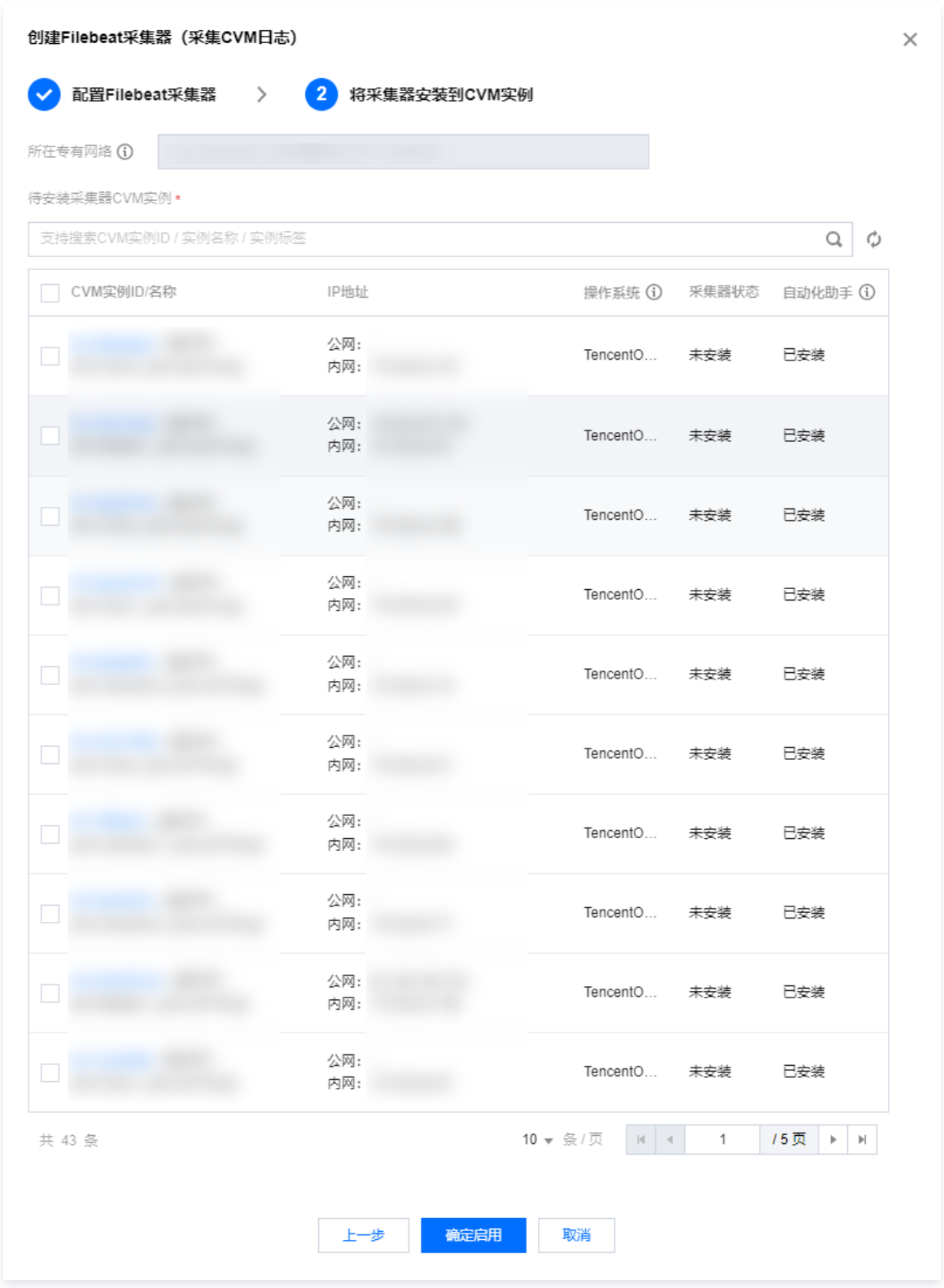
2. 在创建 Filebeat 采集器中，设置采集器信息。

- 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。

- 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。



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

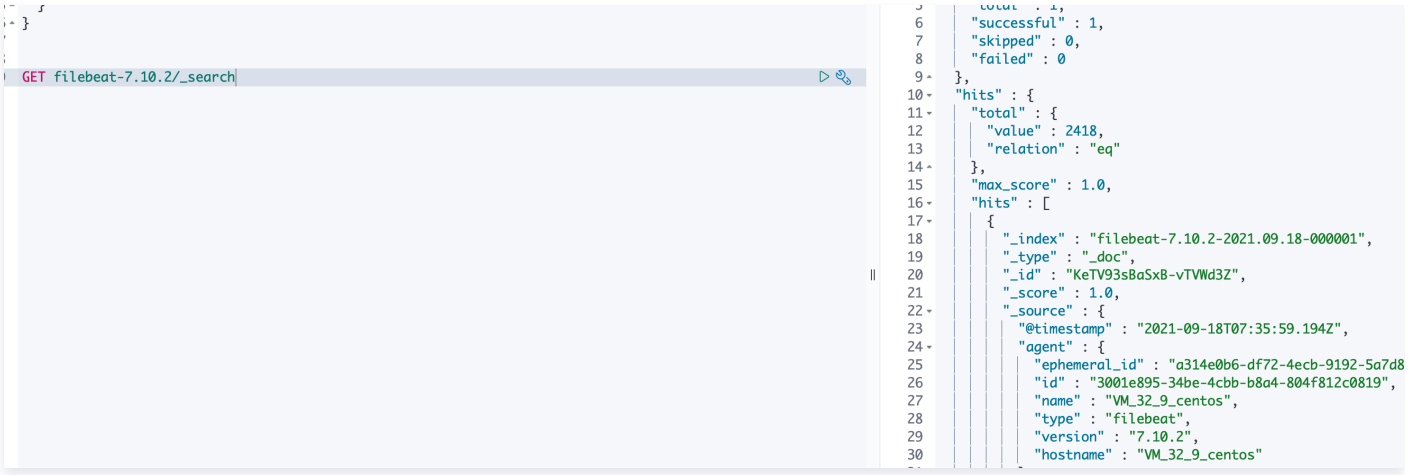
如需将采集的日志数据传送到腾讯云 Logstash 实例，可参考 接收 Filebeat 发送的数据并写入到 Elasticsearch 配置 logstash 管道。

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
```



说明

filebeat-7.14.2为索引名称。

创建 Metricbeat 采集系统数据

Last updated：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 。

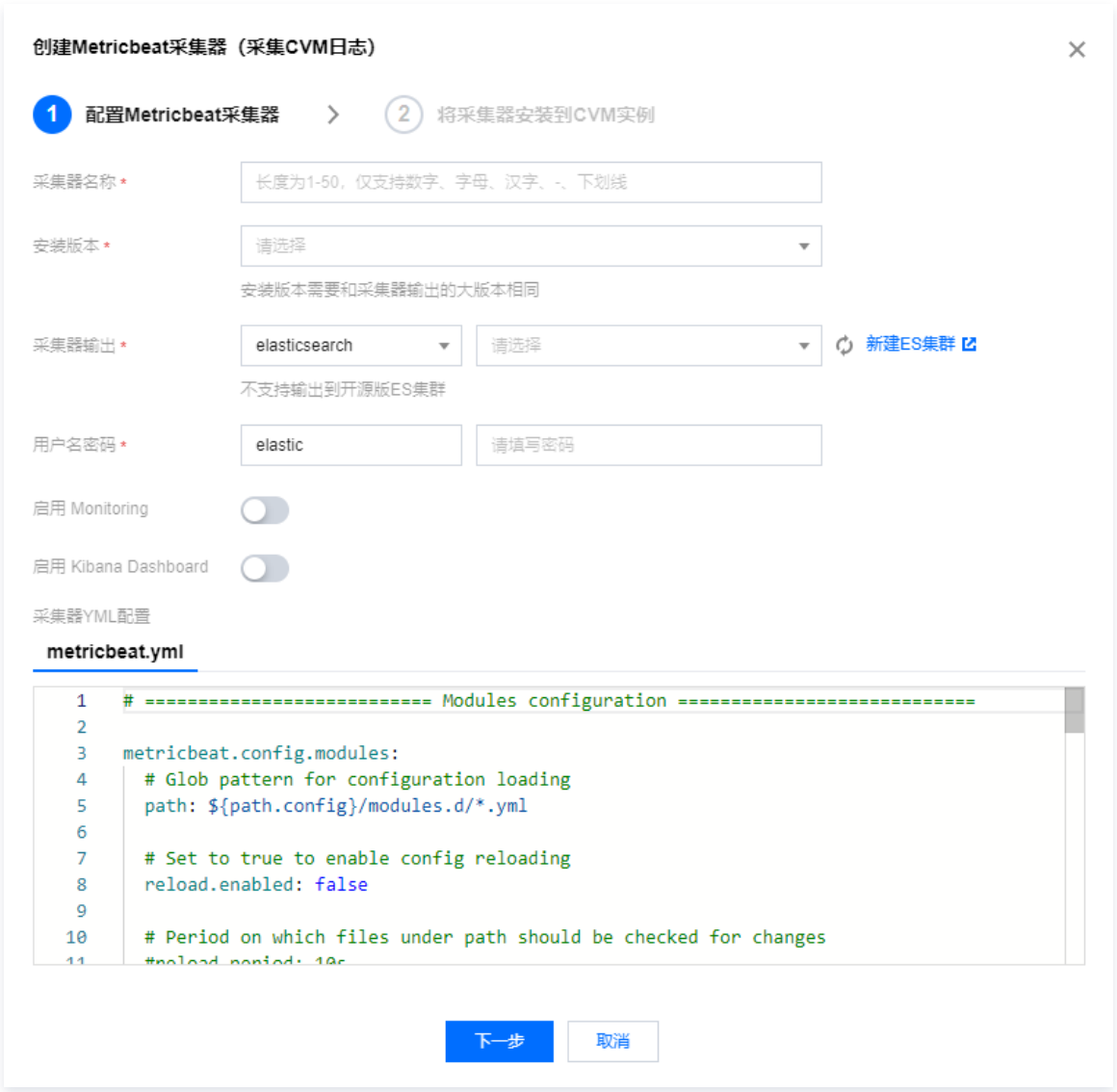
操作步骤

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。

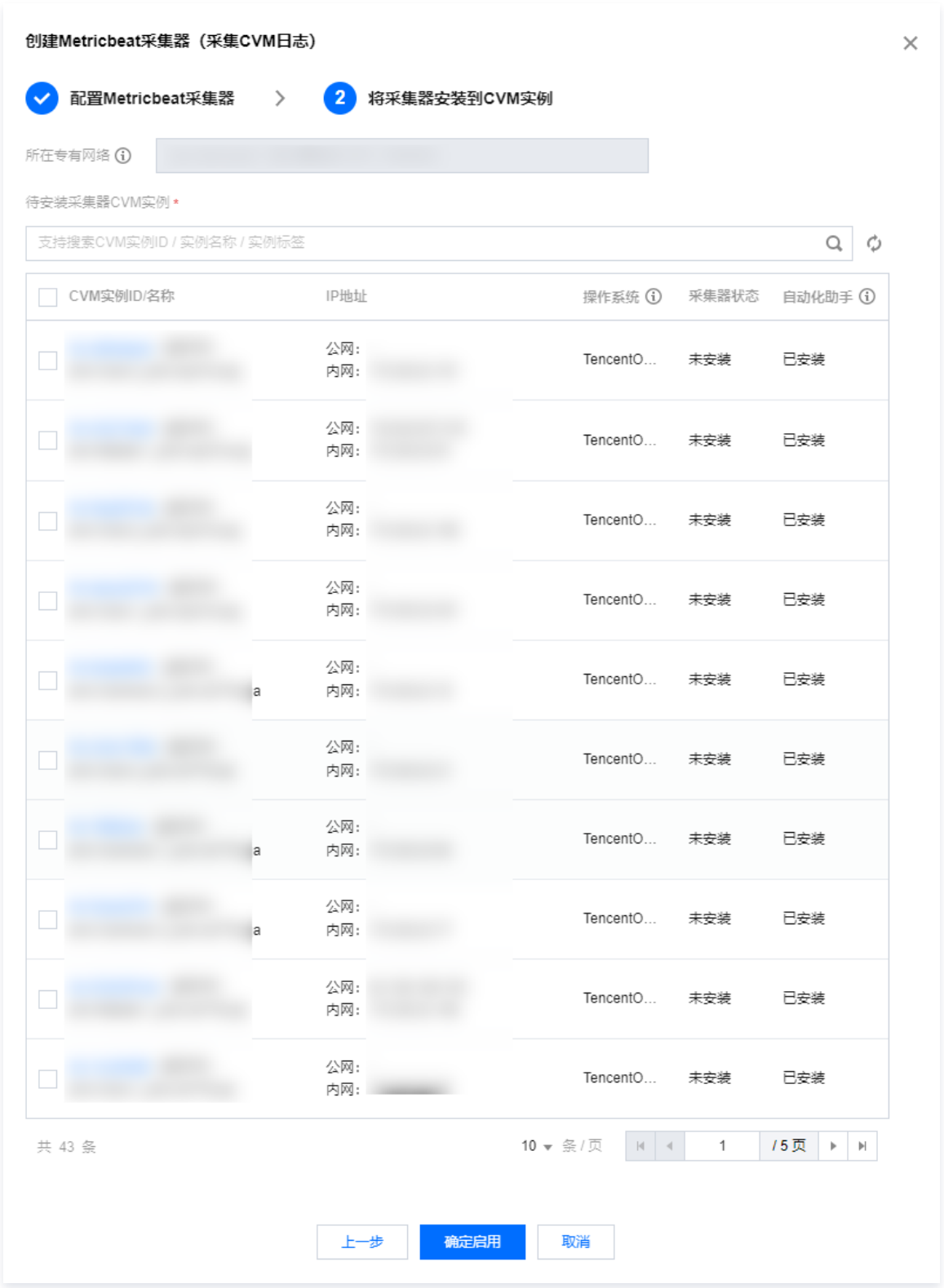
2. 在创建 Metricbeat 采集器中，设置采集器信息。

- 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 。

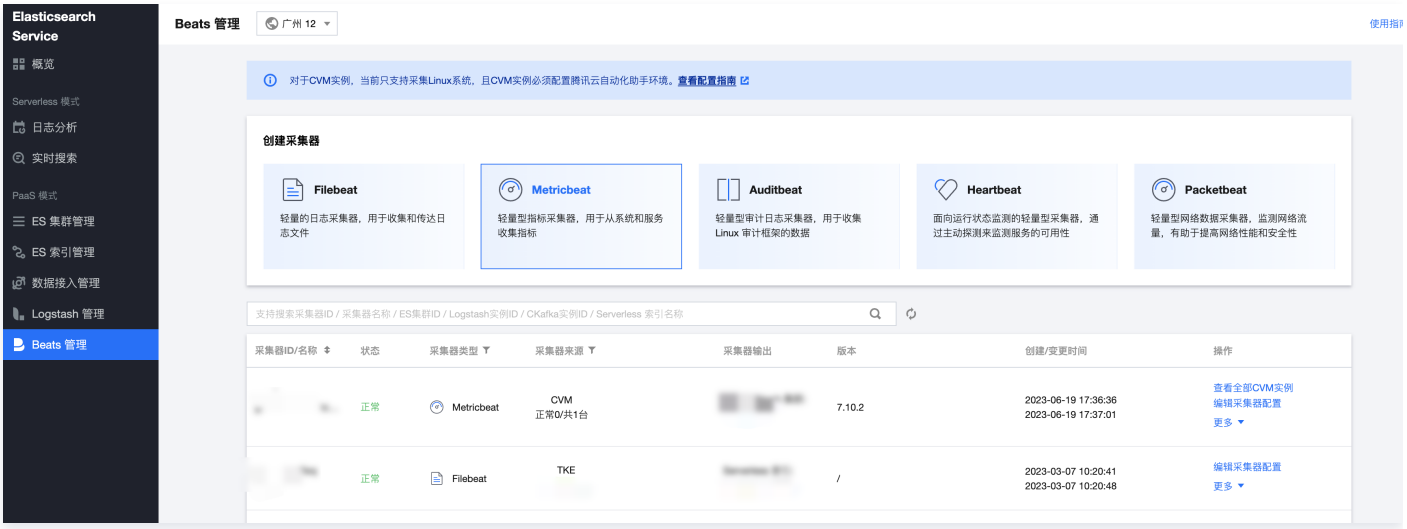


- 将采集器安装到 CVM 实例。选择要安装采集器的 CVM 实例，完成后单击**确定启用**。
  - CVM 必须安装自动化助手，仅支持为已安装自动化助手的 CVM 实例下发采集器配置。

- 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。



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 。



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

Last updated：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

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

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。

2. 在创建 Auditbeat 采集器中，设置采集器信息。

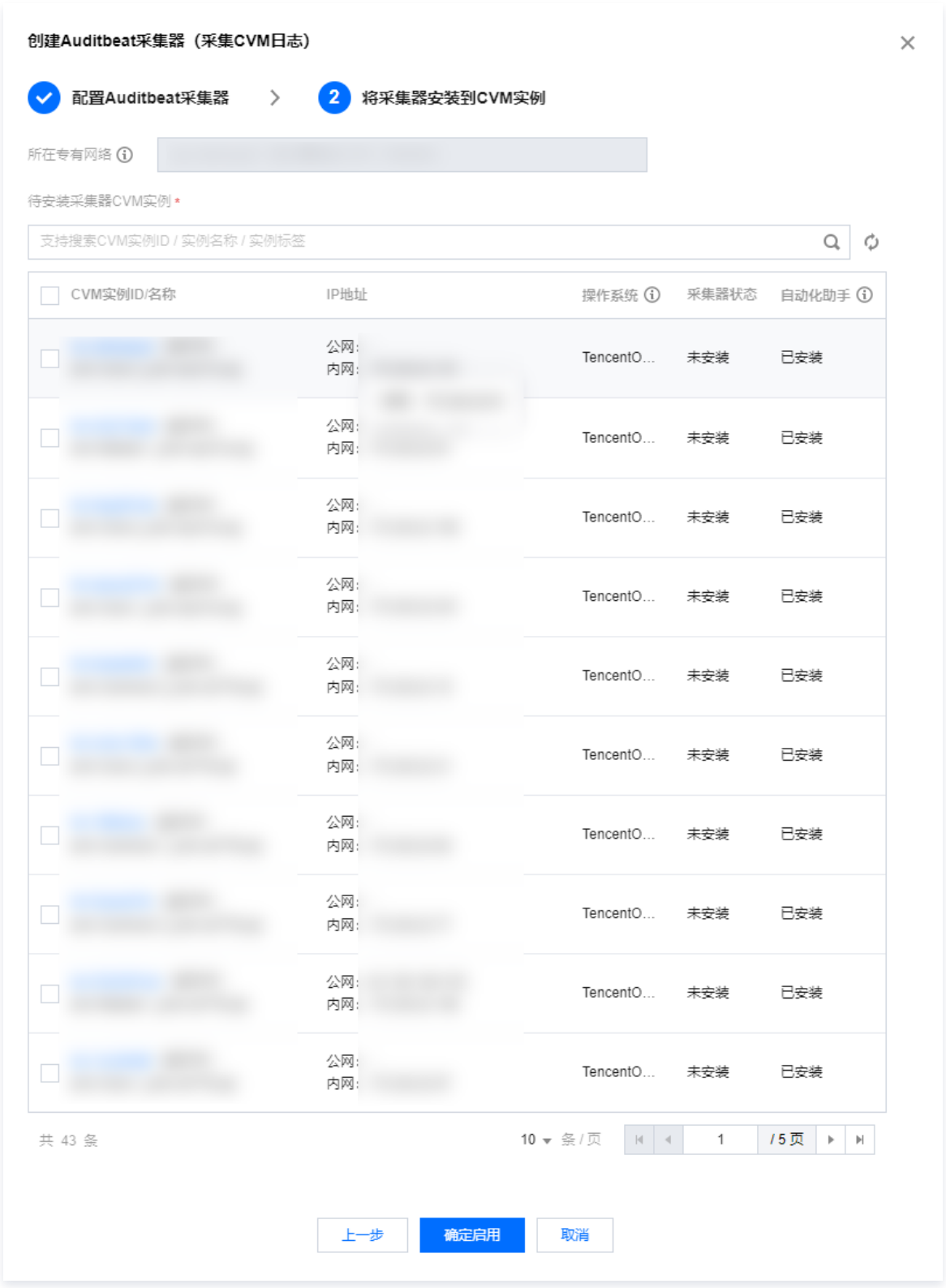
- 配置 Auditbeat 采集器，输入或选择采集器配置信息。完成后单击**下一步**。
  - 采集器名称：自定义采集器的名称，格式为1个 - 50个英文、汉字、数字或下划线（_）。
  - 安装版本：支持6.8.15、7.10.2或7.14.2版本。
  - 采集器输出：采集的数据支持传送到腾讯云 Elasticsearch 与 Logstash 实例，请选择与需采集数据的 CVM 在同一 VPC 下的 ES 集群和 Logstash 实例。不支持输出至开源版 ES 集群。
  - 用户名密码：若选择输出采集数据到开启用户登录认证的 ES 集群，需要填写用户名和密码，使 Auditbeat 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。

- 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。

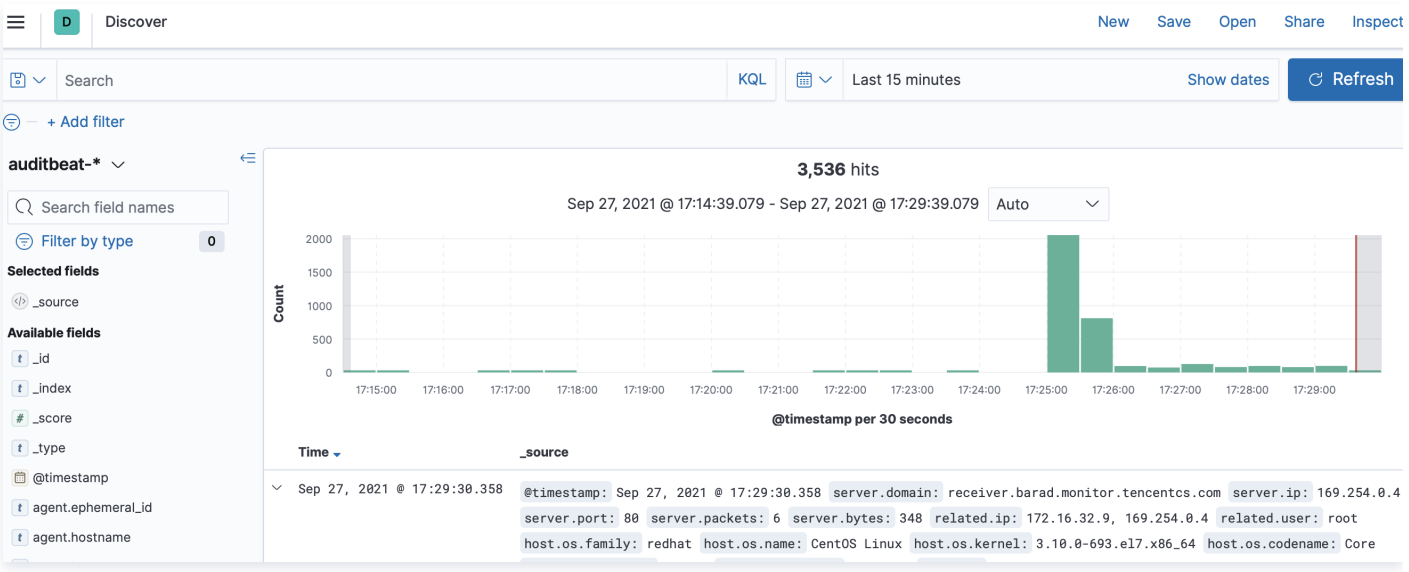
- 仅支持选择和采集器输出在同一 VPC 下的 CVM 实例进行安装，若无法找到目标 CVM 实例，需要更改采集器输出。



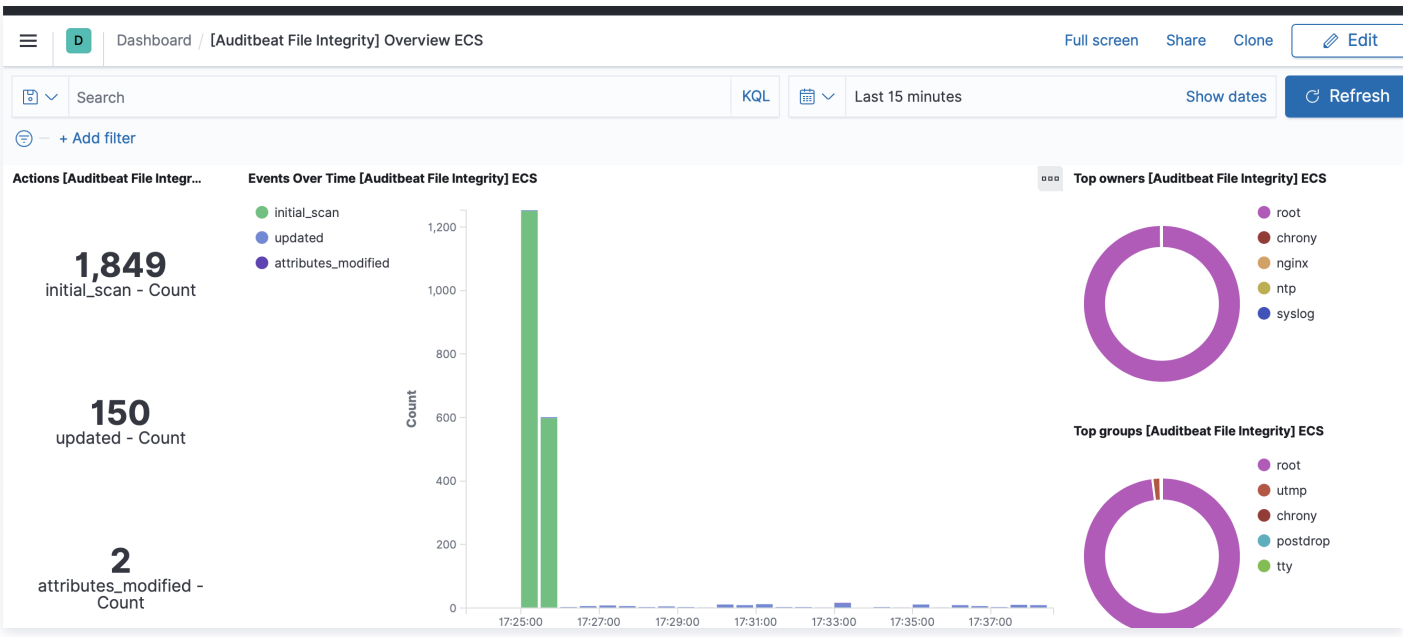
3. 单击**确定启用**后，跳转到 Beats 采集器管理界面，可以查看 Auditbeat 采集器运行状态，显示“正常”则表示采集器安装成功。支持 修改采集器配置 和 管理 CVM 实例 。

Kibana 查看结果

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



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

Last updated：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。

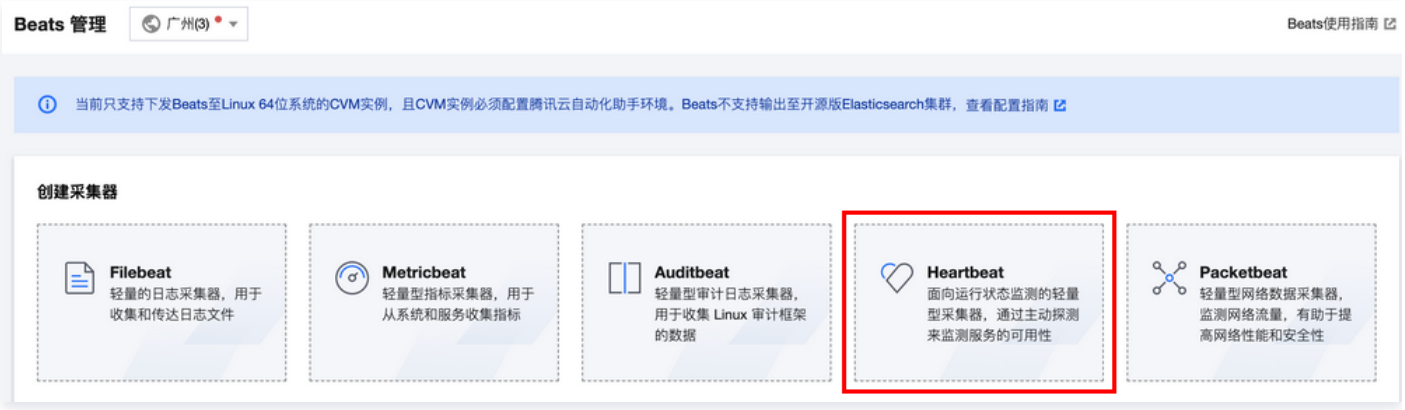
> ⚠ 注意
> Beats 目前仅支持64位的 Linux 操作系统。

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。



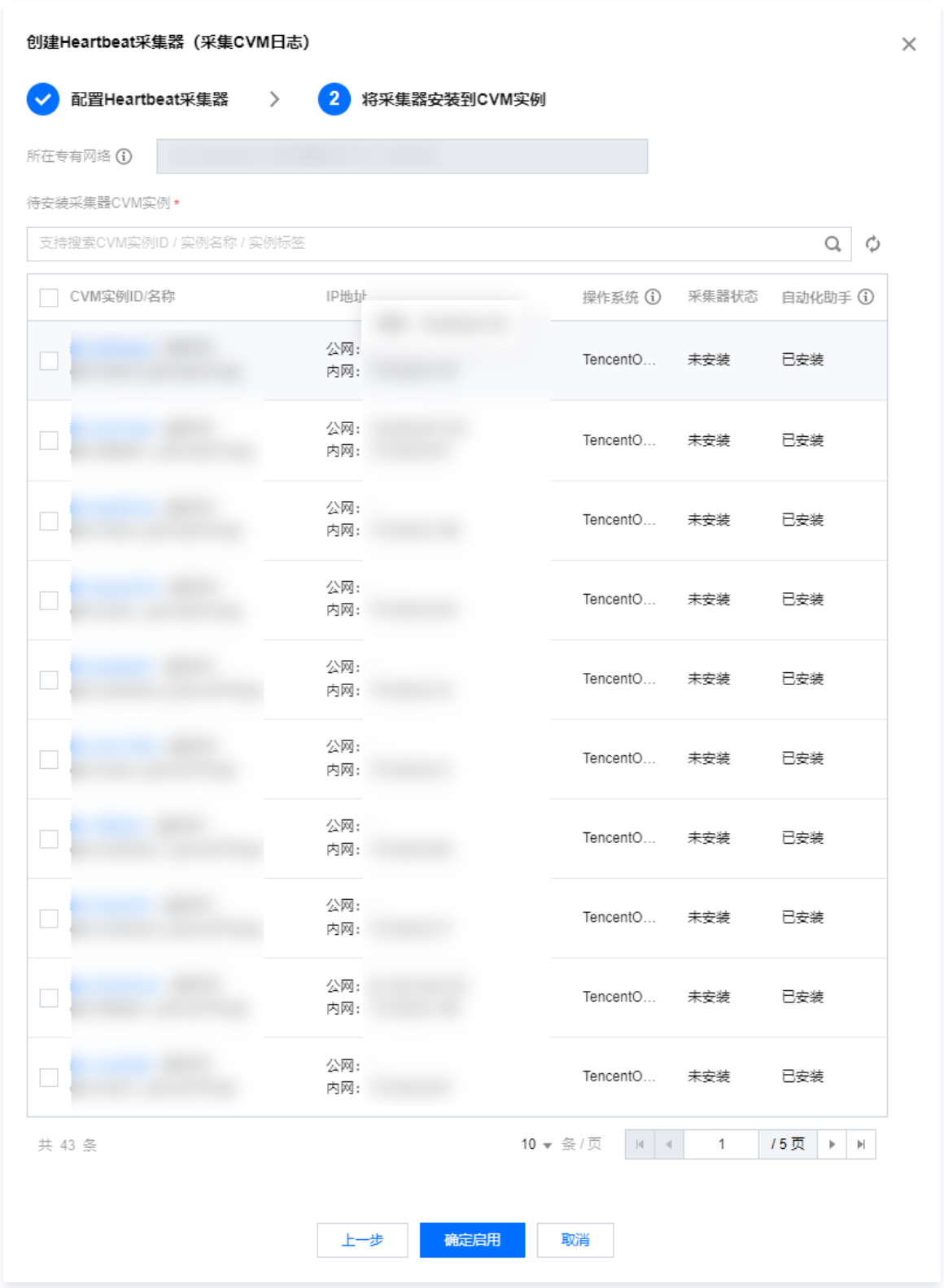
2. 在创建 Heartbeat 采集器中，设置采集器信息。

- 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。

- 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。



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。

创建 Packetbeat 采集网络流量

Last updated：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。

> ⚠ **注意**
> Beats 目前仅支持64位的 Linux 操作系统。

- 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

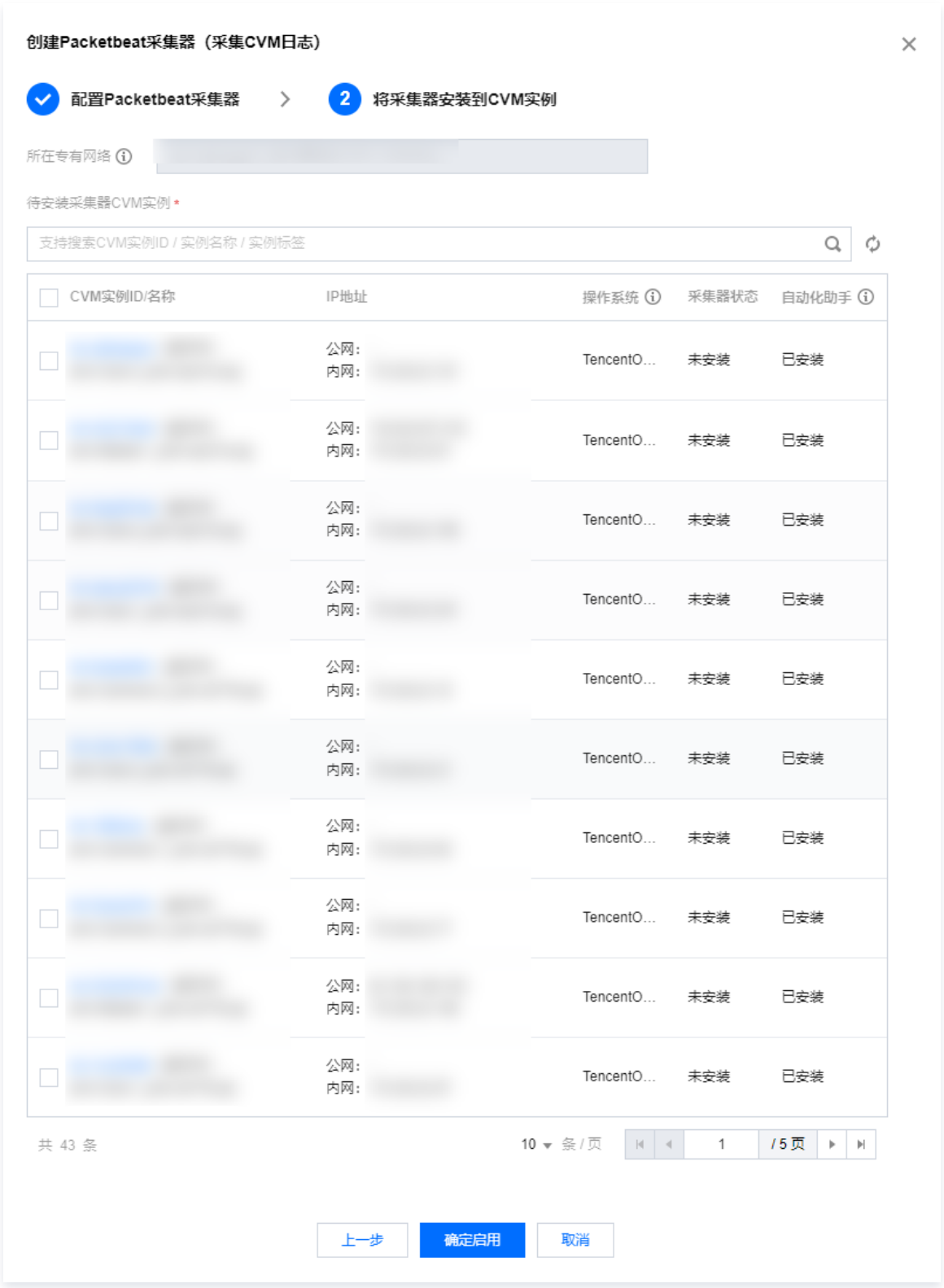
1. 登录 Elasticsearch Service 控制台 Beats 管理界面，并授权服务相关角色，单击创建 **Packetbeat** 采集器。

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 。

- 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。

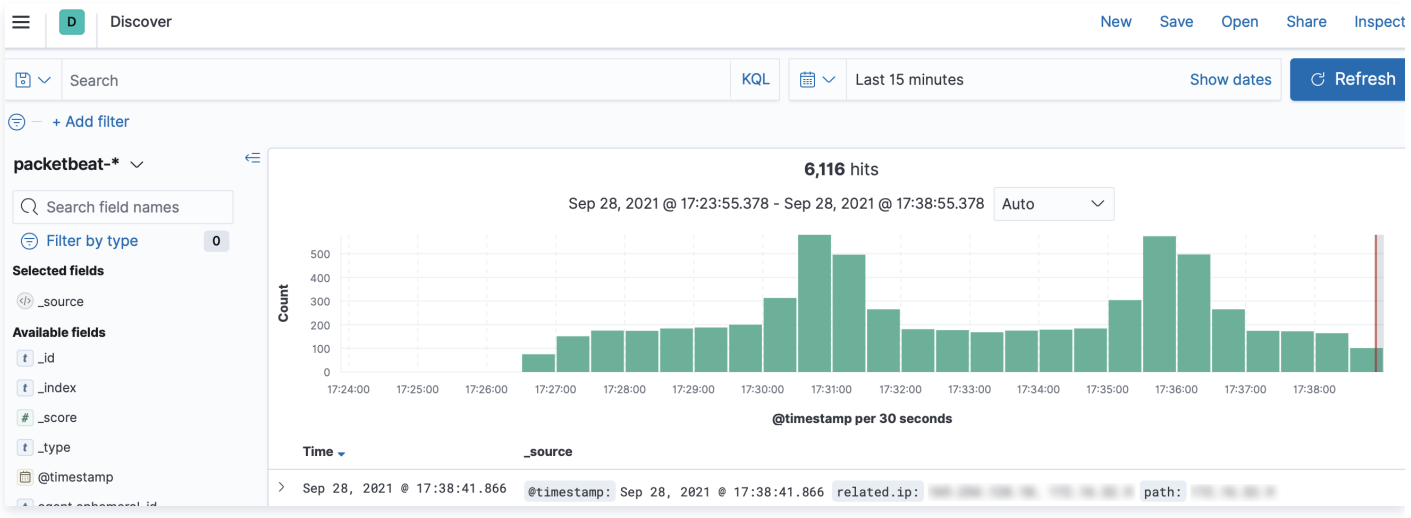


3. 单击**确定启用**后，跳转到 Beats 采集器管理界面，可以查看 Packetbeat 采集器运行状态，显示“正常”则表示采集器安装成功。支持 修改采集器配置 和 管理 CVM 实例 。

Kibana 查看结果

1. 登录腾讯云 Kibana 控制台。

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



管理 CVM 实例

Last updated：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。

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。

通过 Filebeat 采集 TKE 容器日志

Last updated：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。

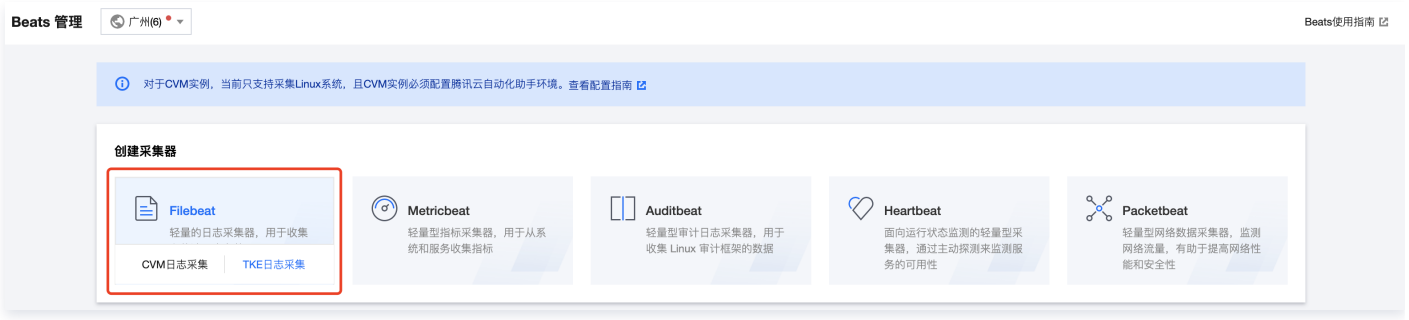
操作须知

- 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**。



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：

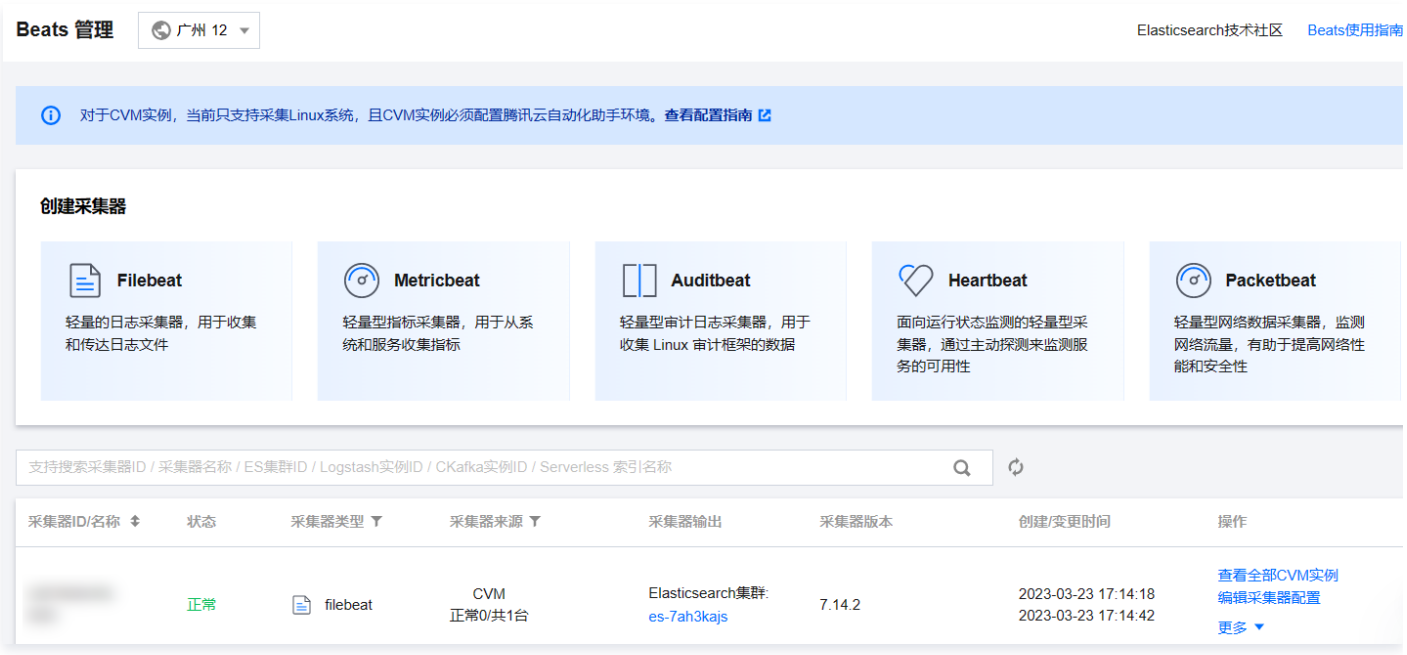
   - 采集器名称：必填。自定义采集器的名称。
   - 安装版本：必选。支持6.8.21、7.10.2、7.14.0、7.17.1，安装版本需要和**采集器输出**的大版本相同。
   - 采集器输出：必选。采集的数据支持传送到腾讯云 Elasticsearch 集群与 Logstash 实例，请选择与需采集数据的 TKE 在同一 VPC 下的 ES 集群和 Logstash 实例。不支持输出至开源版 ES 集群。
   - 用户名密码：必填。若选择输出采集数据到开启用户登录认证的 ES 集群，需要填写用户名和密码，使得 Filebeat 有权限向 ES 集群中写入数据。用户名默认为 elastic，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。

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、过滤等，一般采用默认配置，详情请参见 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。



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 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
```