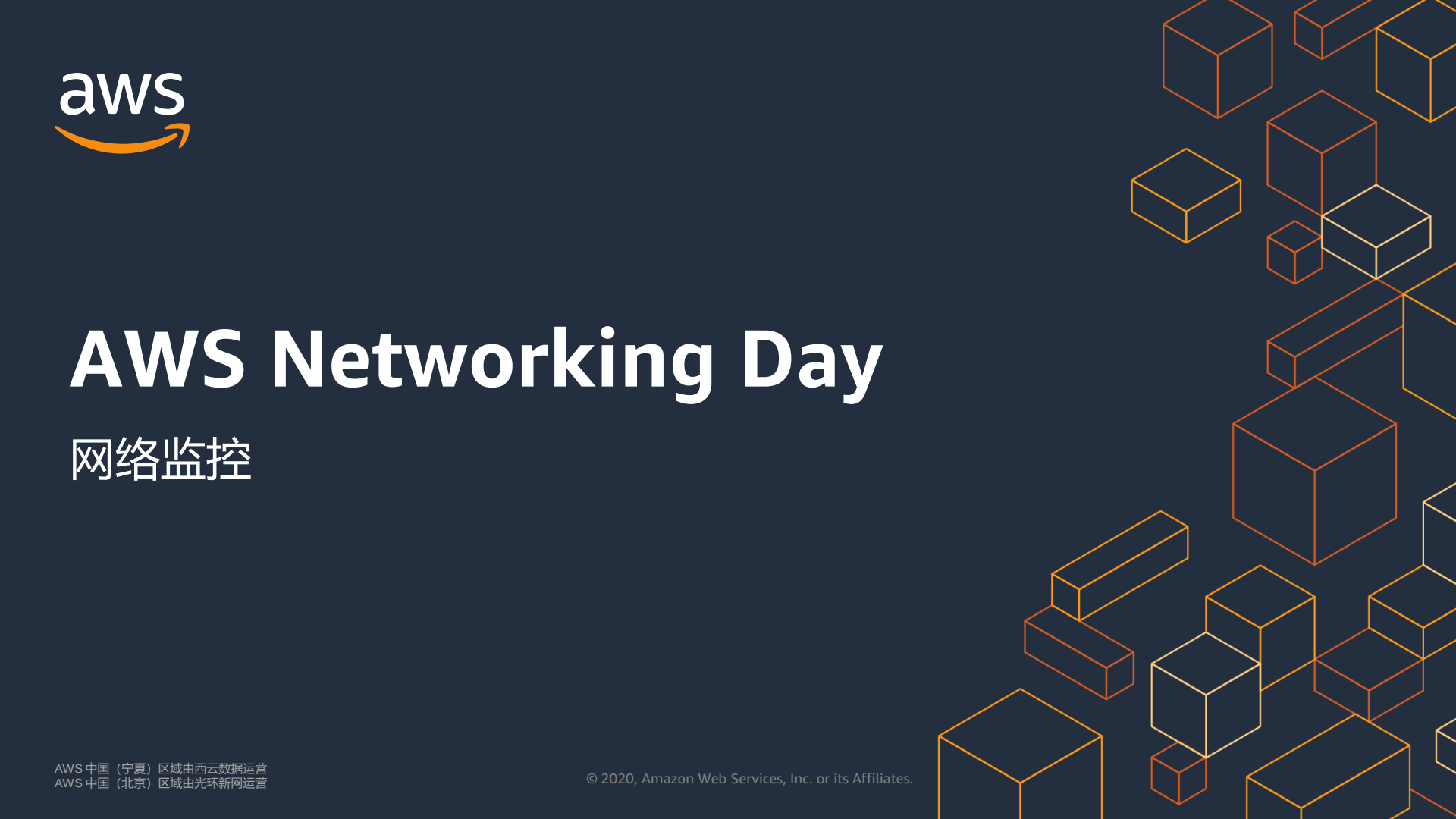


AWS Networking Day

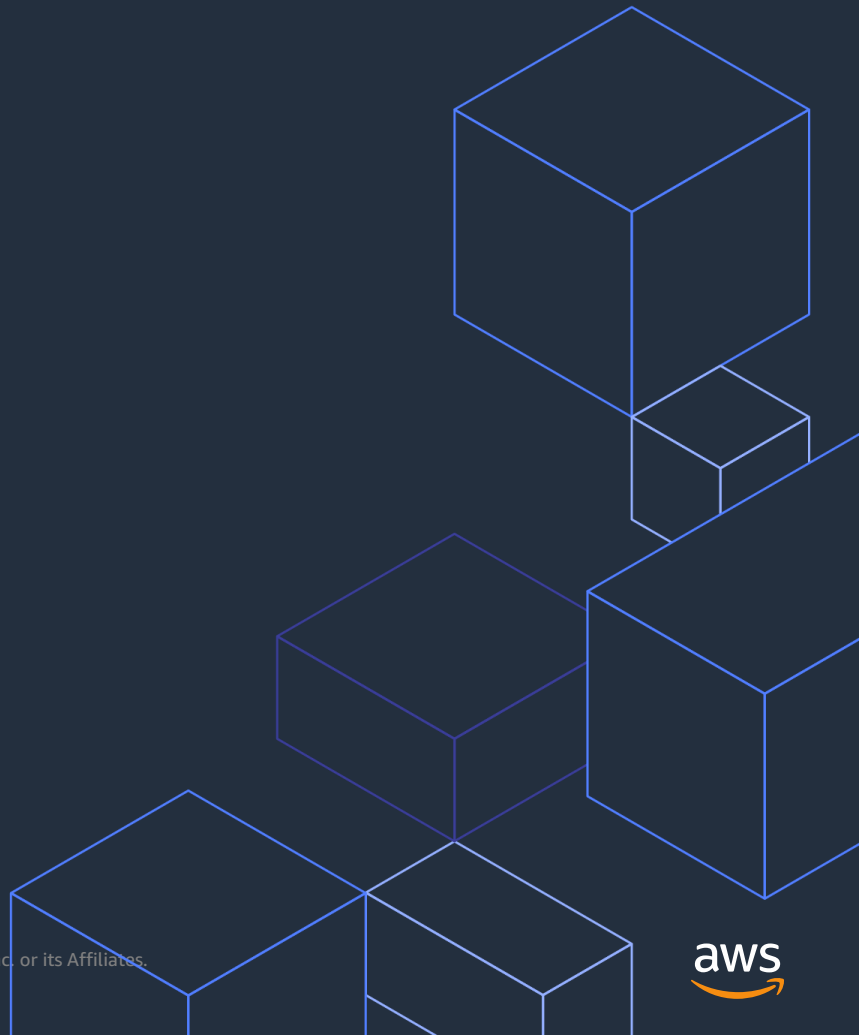
网络监控

AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

Agenda – 网络监控

- 监控流量
- 事件通知和自动化
- API 活动的监控

流量监控



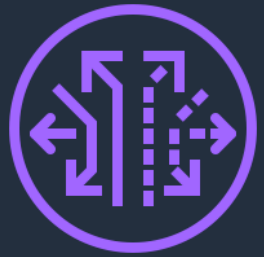
AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

aws

流量监控的选择

VPC 流量日志（Flow Logs）

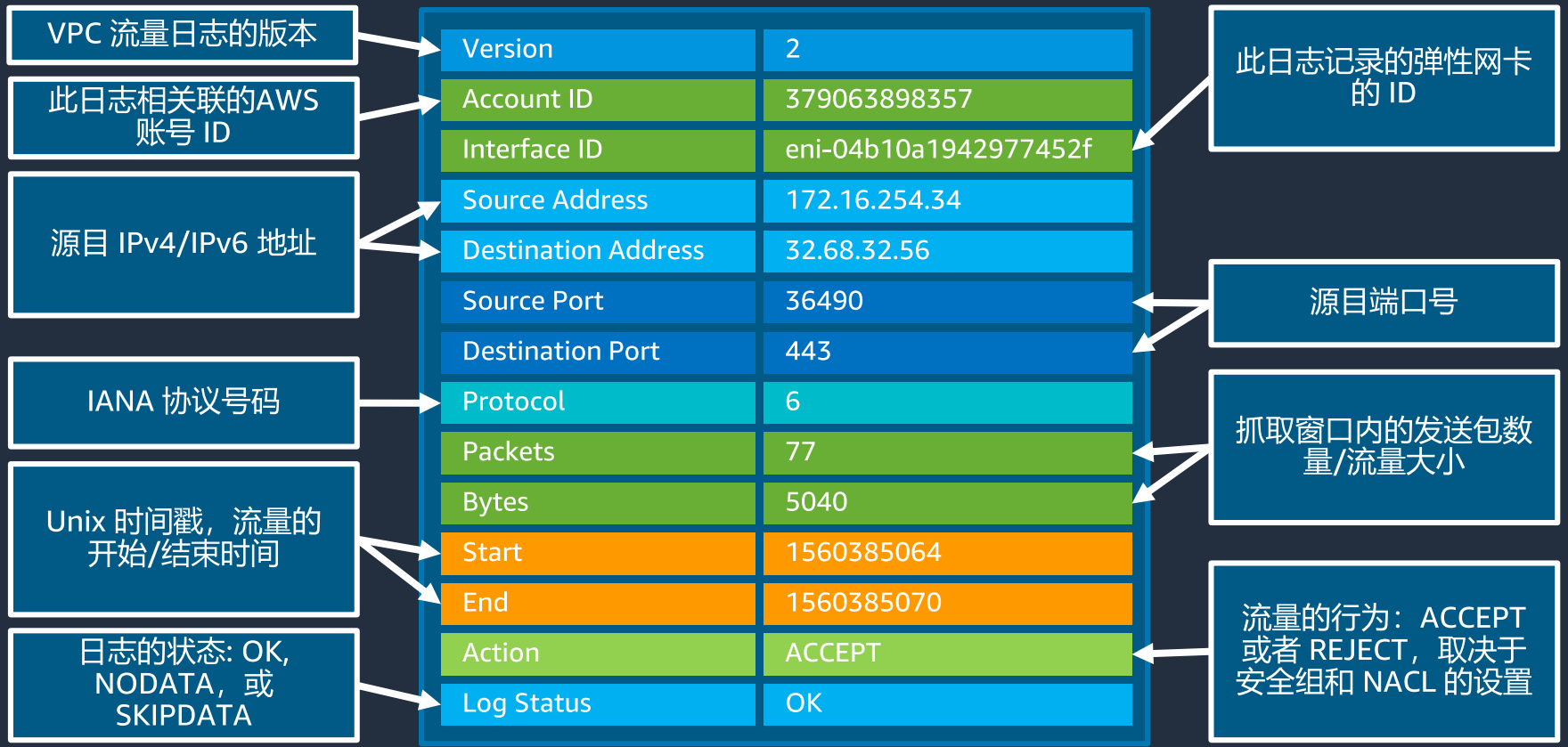
收集和保存 IP 头部信息



流量镜像（Traffic Mirroring）

复制一份流量，包含数据报文信息

解析 VPC 流量日志



解析 VPC 流量日志

除了 IP 标头信息，你还可以添加其他元数据信息，例如：

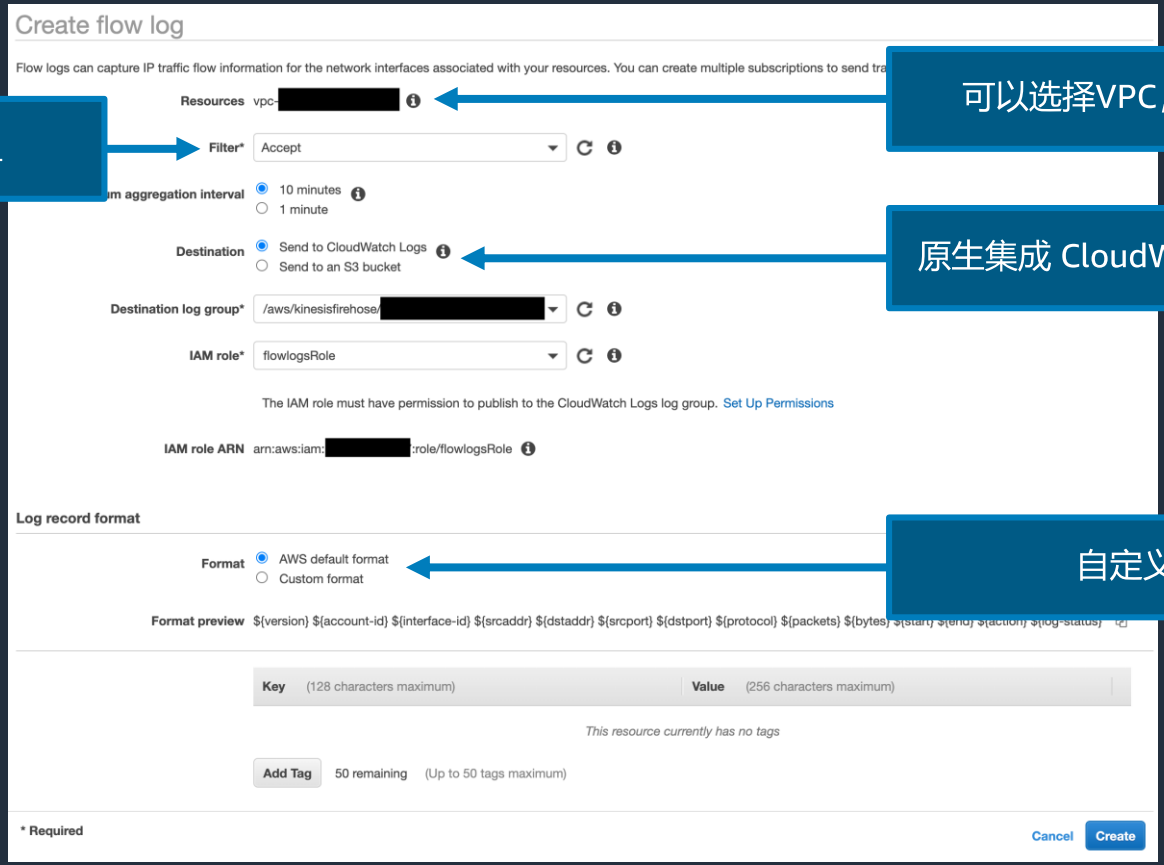
VPC id
Subnet id
Instance id
TCP Flags (SYN, ACK, FIN)
Type (IPv4, IPv6)
Packet Source Address
Packet Destination Address

Packet Source/Destination Address 是网络中介的 IP 地址，例如 NAT 网关

https://aws.amazon.com/blogs/aws/learn-from-your-vpc-flow-logs-with-additional-meta-data/

如何创建 VPC 流量日志

选择流量状态是 Accept，Rejected 还是包含两者



可以选择VPC，子网和网卡

原生集成 CloudWatch 日志和 S3

自定义格式

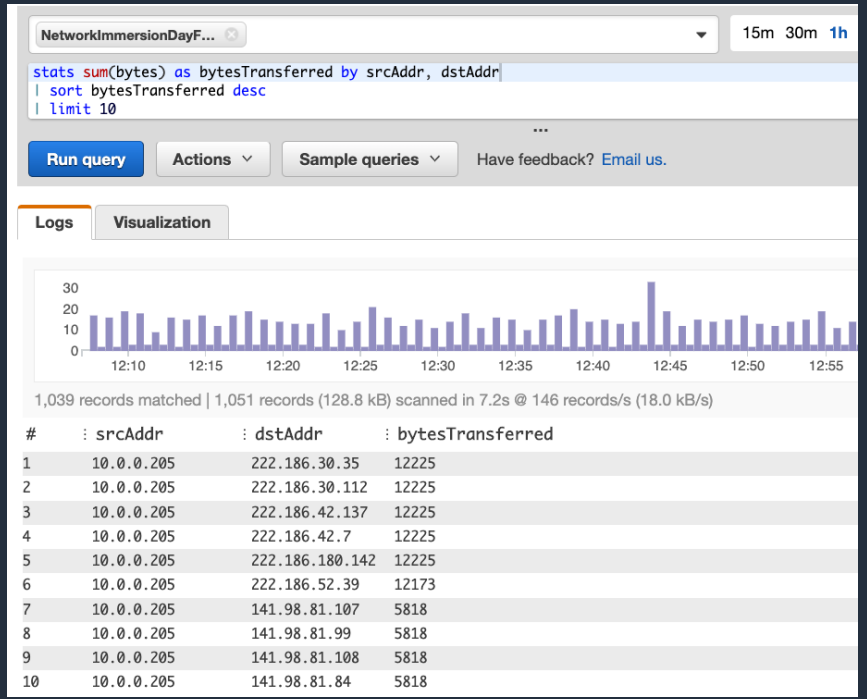
分析 VPC 流量日志

CloudWatch Logs Insights

交互式地搜索和分析日志数据，可视化所有结果，更好地响应运维问题。

内嵌的查询例子：

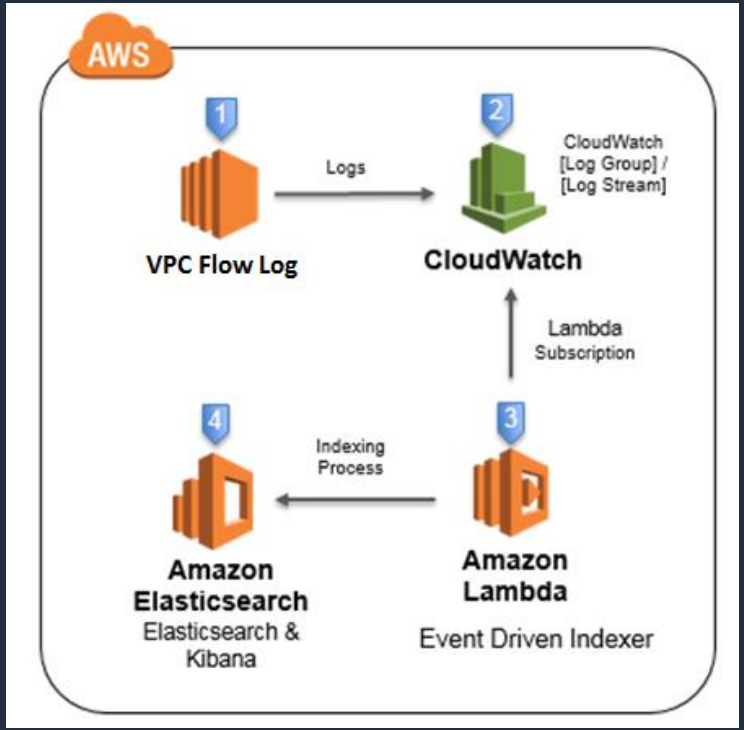
- 传输字节数最多的10大源目 IP 地址（如右图所示）
- 被拒绝的请求最多的前20个源IP地址
- 使用 UDP 传输协议的 IP 地址
- 按源和目标 IP 地址列出的平均、最小和最大传输字节数



#	srcAddr	dstAddr	bytesTransferred
1	10.0.0.205	222.186.30.35	12225
2	10.0.0.205	222.186.30.112	12225
3	10.0.0.205	222.186.42.137	12225
4	10.0.0.205	222.186.42.7	12225
5	10.0.0.205	222.186.180.142	12225
6	10.0.0.205	222.186.52.39	12173
7	10.0.0.205	141.98.81.107	5818
8	10.0.0.205	141.98.81.99	5818
9	10.0.0.205	141.98.81.108	5818
10	10.0.0.205	141.98.81.84	5818

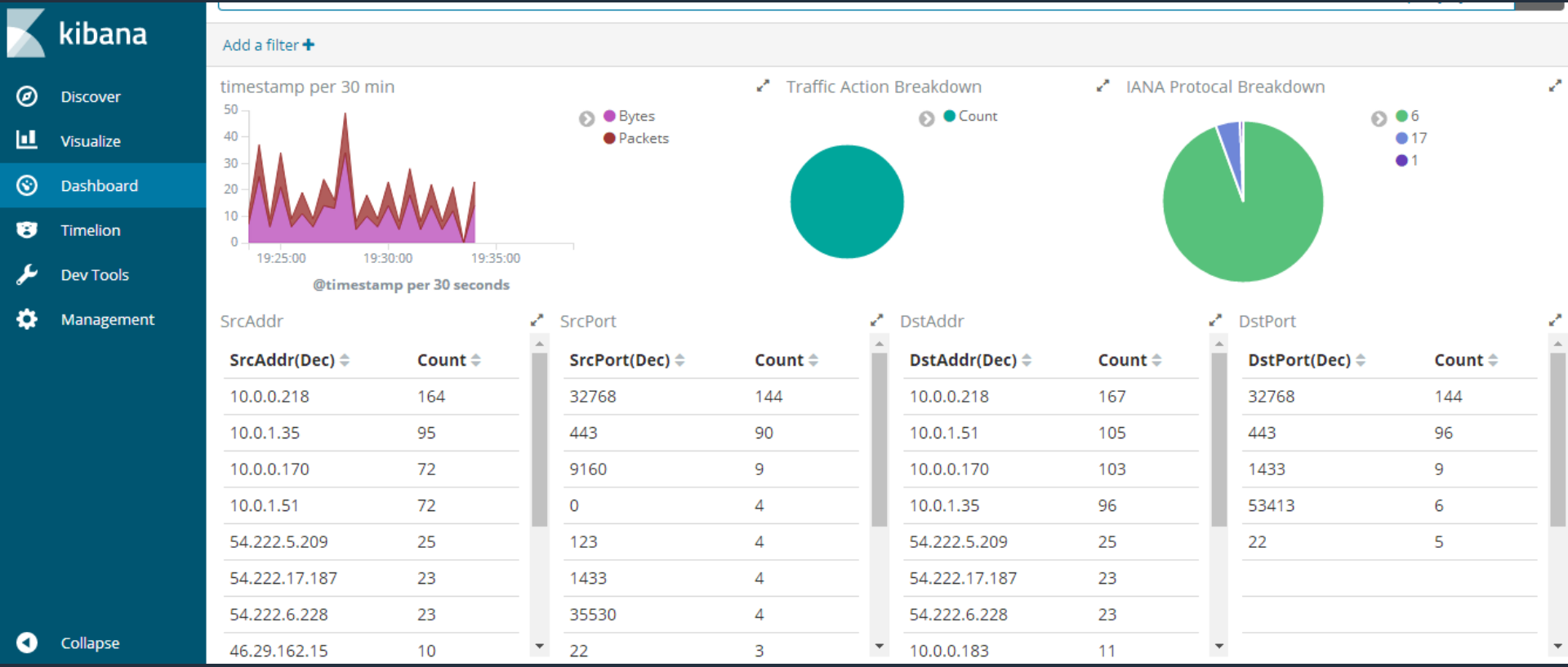
VPC 流日志集成 Amazon ElasticSearch

1. 将 VPC 流日志写入 CloudWatch 日志组
2. CloudWatch 日志触发 Lambda 函数
3. 日志内容通过 Lambda 函数注入 ES 中
4. ES 进行可视化展现



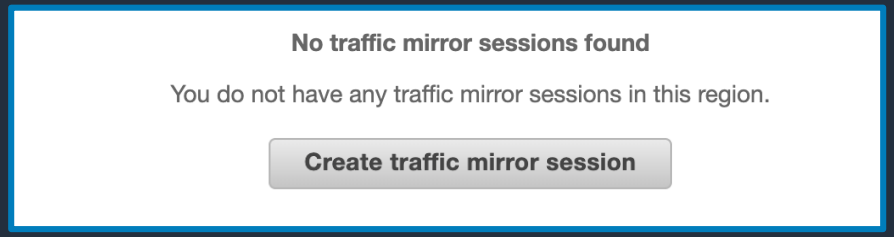
https://amazonaws-china.com/cn/blogs/china/amazon-elasticsearch-service-vpc/

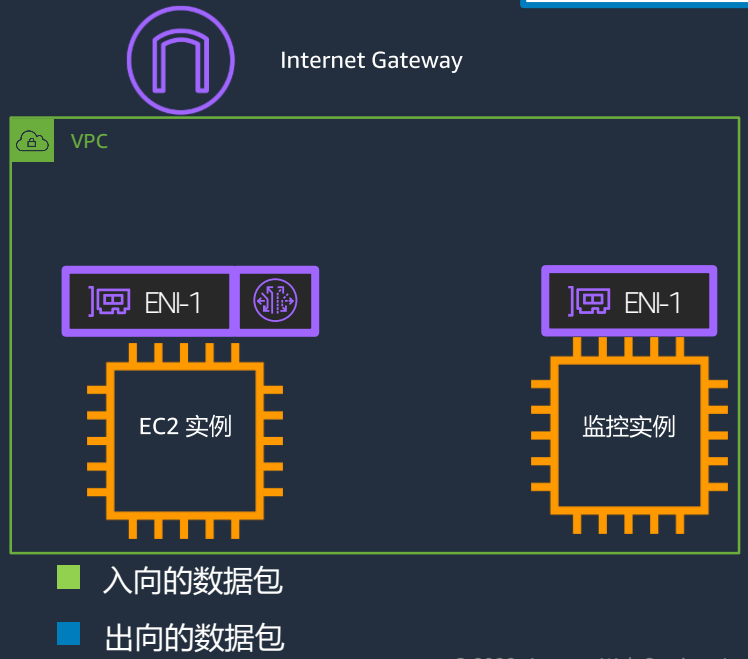
VPC 流日志集成 Amazon ElasticSearch



aws

VPC 流量镜像





打造自己的流量分析器

开源的流量分析工具

AWS 流量镜像合作伙伴工具

AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

VPC 流量镜像：3个元素

目标

被镜像的流量去往的目的地

过滤器

在一个流量镜像会话中，需要定义一系列的过滤规则

会话

一个会话记录了过滤器，源和目的

提供流量镜像工具的合作伙伴

Flowmon Networks

AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

aws

提供流量镜像工具的合作伙伴

Big Switch Networks

Fidelis
Cybersecurity

AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

aws

流量监控的使用场景

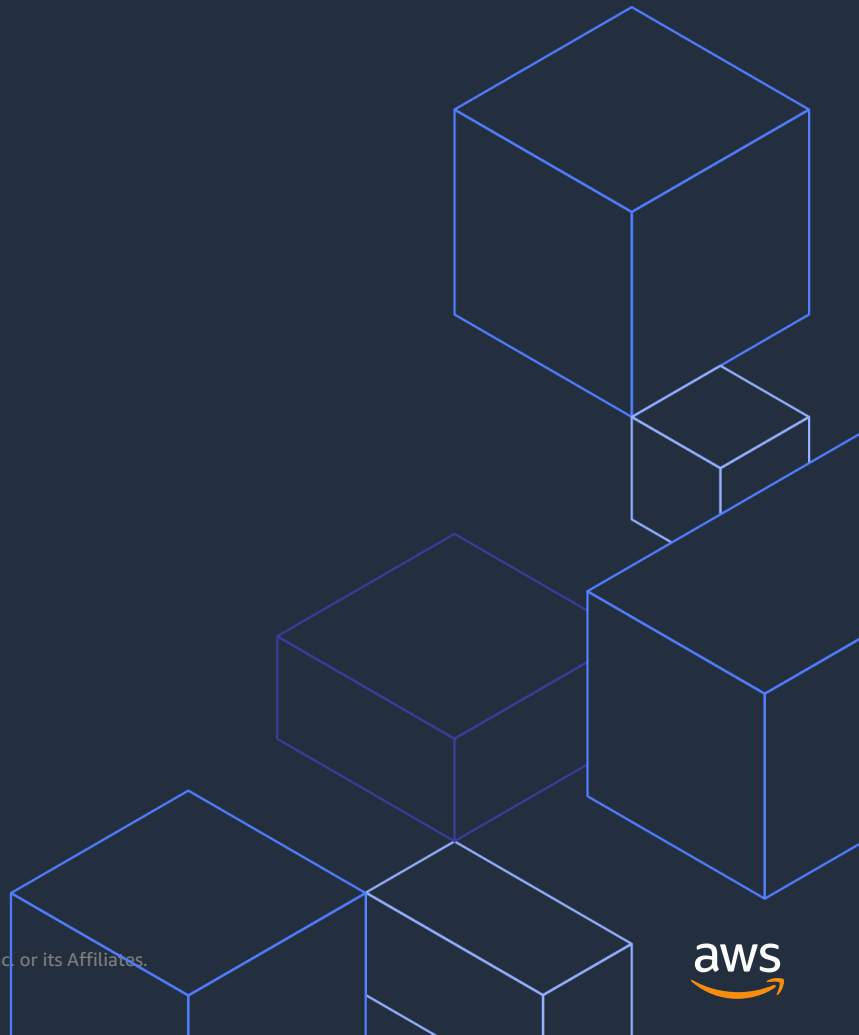
VPC 流量日志

- 分析特别严格的安全组规则
- 监控访问实例的流量
- 判断进出网卡的流量方向

流量镜像

- 内容检查
- 威胁监控
- 故障排查

事件通知和自动化



应用和基础架构的监控

CloudWatch 指标

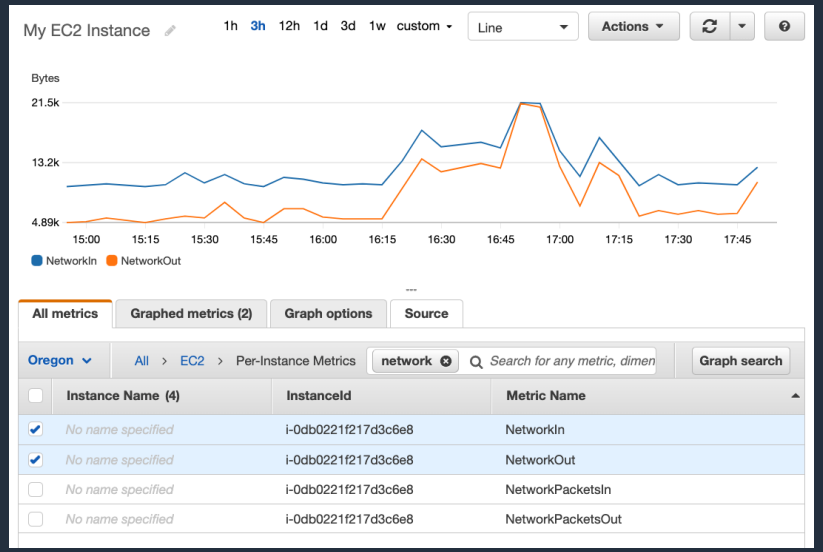
自动收集超过70个 AWS 服务的默认监控指标

CloudWatch 告警

设置指标的阈值，并且触发一个动作(比如电话/邮件告警)

使用 CloudWatch 监控核心指标

EC2 Instance	NetworkIn
	NetworkOut
	NetworkPacketsIn
	NetworkPacketsOut
Shield Advanced	DDoSDetected
	DDoSAttackBitsPerSecond
	DDoSAttackPacketsPerSecond
	DDoSAttackRequestsPerSecond
WAF	BlockedRequests



- NLB 和 ALB 各有超过13种指标
- 所有监控指标数据可以直接在 CloudWatch 面板上看到

aws

使用 CloudWatch 监控核心指标

VPN	State
	DataIn
	DataOut

VIF	VirtualInterfaceBpsIngress
	VirtualInterfaceBpsEgress
	VirtualInterfacePpsIngress
	VirtualInterfacePpsEgress

Direct Connect	ConnectionState
	ConnectionBpsIngress
	ConnectionBpsEgress
	ConnectionPpsIngress
	ConnectionPpsEgress
	ConnectionLightLevelTx
	ConnectionLightLevelRx
	ConnectionCRCErrorCount

Transit Gateway	BytesIn
	BytesOut
	PacketsIn
	PacketsOut
	BytesDropCountNoRoute
	BytesDropCountBlackhole
	PacketDropCountNoRoute
	PacketDropCountBlackhole

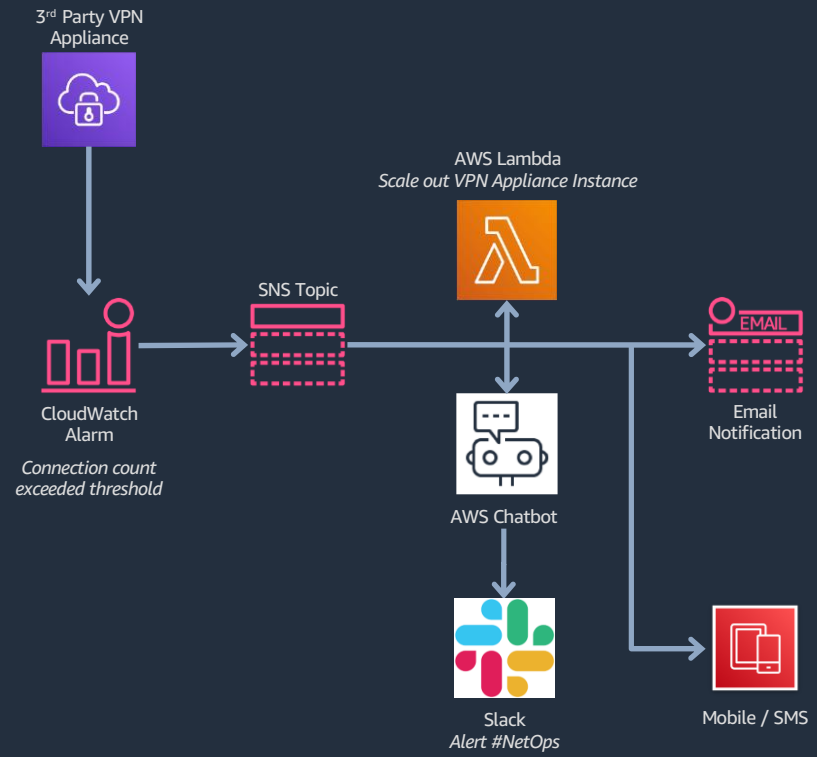
你也可以使用 AWS CLI 或者 API 将自定义的指标推送到 CloudWatch 上，比如推送第三方防火墙的指标

aws

使用 CloudWatch 告警进行自动响应

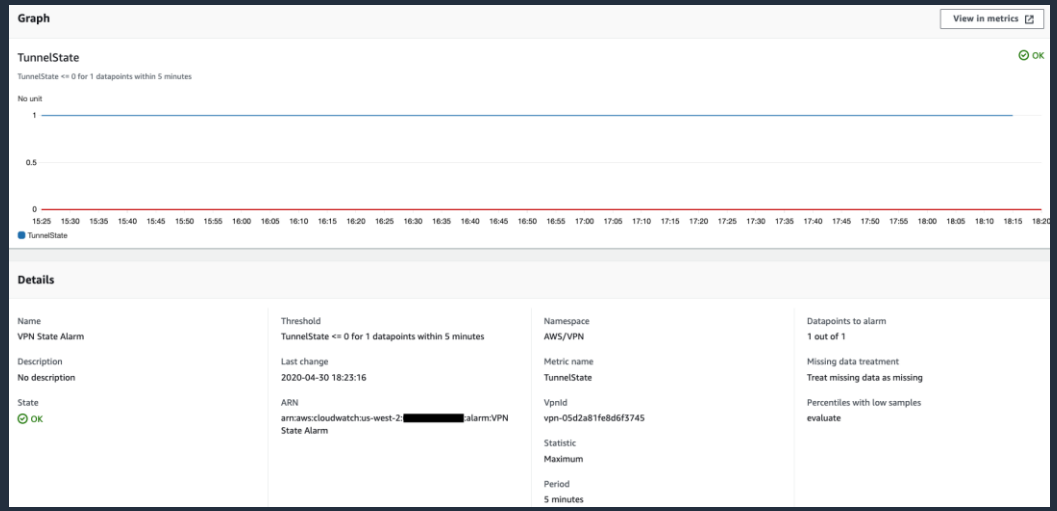
指标超过阈值之后能触发的动作有：

- 向Slack，微信，钉钉，邮件，短信等发送消息
- 触发灾难恢复机制
- 更新安全组设置
- 对流量异常进行响应
- 自动扩展/收缩第三方防火墙容量
- 触发第三方防火墙的故障转移



如何创建 CloudWatch 告警

- 选择你需要监控的*指标*
- 设置*指标的阈值*，比如大于/大于等于/小于等于/小于某一个值
- 定义什么*告警状态*会触发下一步动作，状态包括：告警中，OK，数据不足
- 选择一个会收到通知的 *SNS 主题*
- （可选）：创建一个告警触发之后要执行的一个 pipeline （即一系列动作）



CloudWatch 指标和告警使用场景

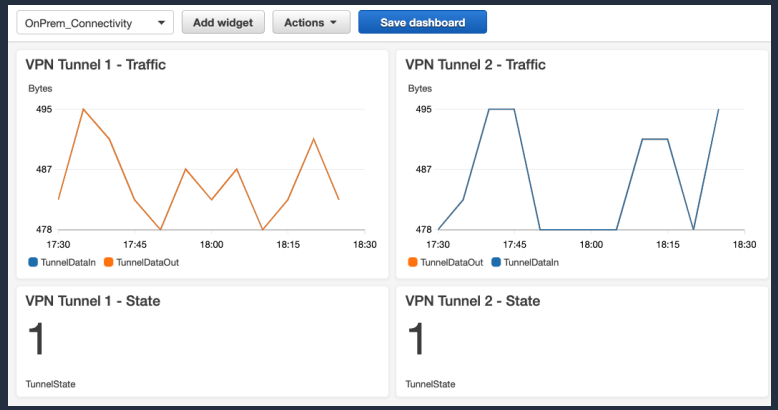
CloudWatch 指标

- 监控多个 AWS 服务的进出包速率和流量速率
- 监控 DDoS 和网络攻击行为
- 监控 VPC 和 Direct Connect 专线的状态

CloudWatch 告警

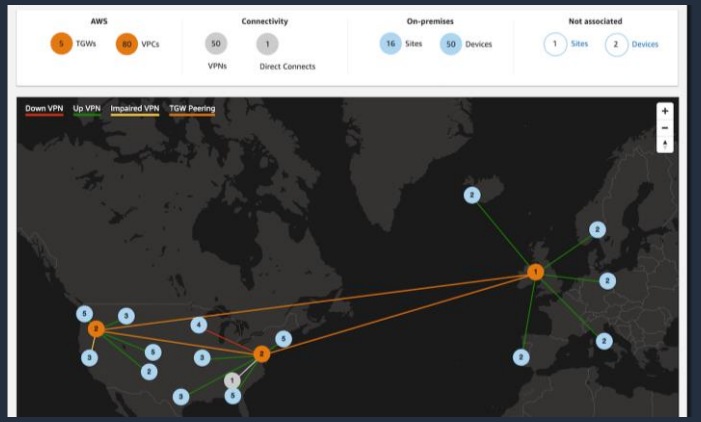
- VPN 和 Direct Connect 专线线路状态变化时候通知你
- 流量异常时候的告警

将网络状态和性能可视化



CloudWatch 面板

让你创建云资源内所有网络指标的图表，支持跨区域和跨 AWS 账号



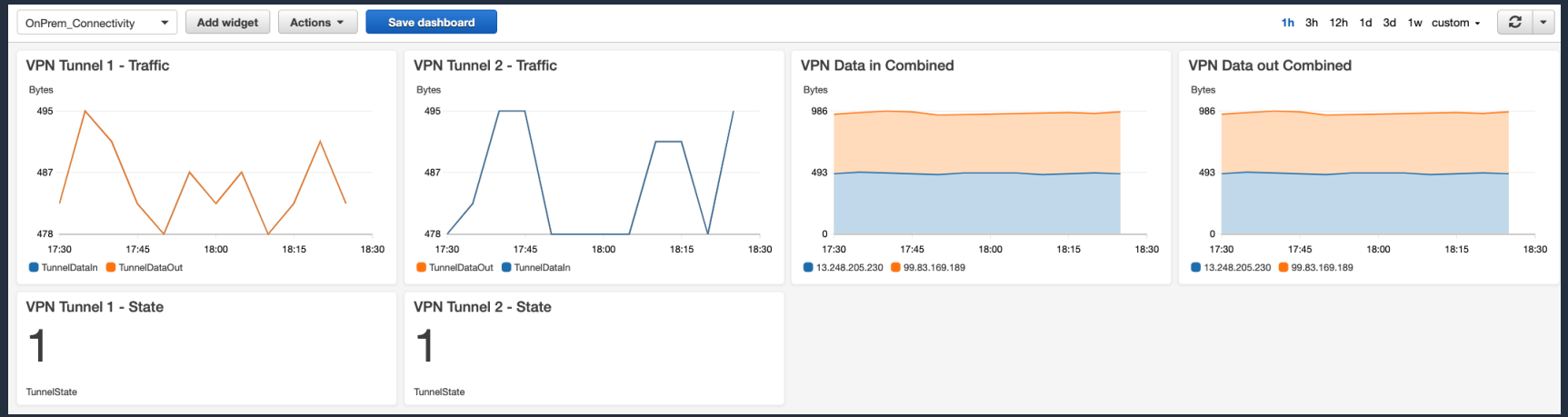
Transit Gateway 网络管理器

提供一个统一的面板来查看你的全球私有网络

aws

如何创建一个定制化的面板

- 创建一个新的*定制化面板*
- 选择要添加的*插件*的类型：线性图，堆叠区域图，数字，文字， Query Result
- 选择你要添加的*指标*
- 将插件放置到面板中



使用网络管理器中央化管理全球网络

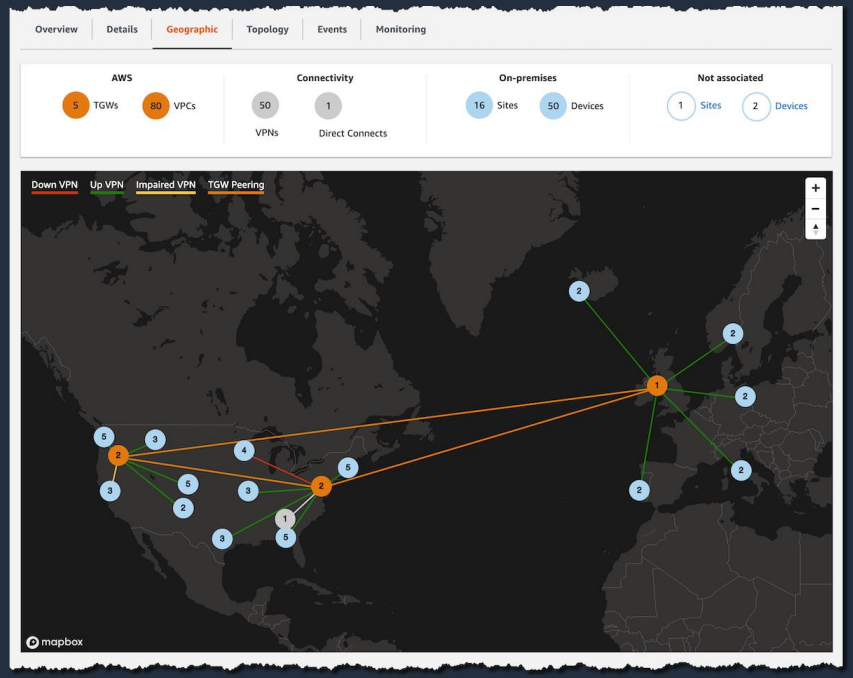
可以与 Transit Gateway 一起使用

可视化：跨 AWS 和本地数据中心的全球网络面板

- Geographic view –网络连接和资源的地图展现
- Topology view – 资源和网络的逻辑关联关系

监控：CloudWatch 的指标和事件

- 指标 – TGW 和 attachment 级别的每秒数据流入/流出和丢包信息
- 事件 – 拓扑变化，状态更新，路由更新



CloudWatch 面板和 TGW 网络管理器使用场景

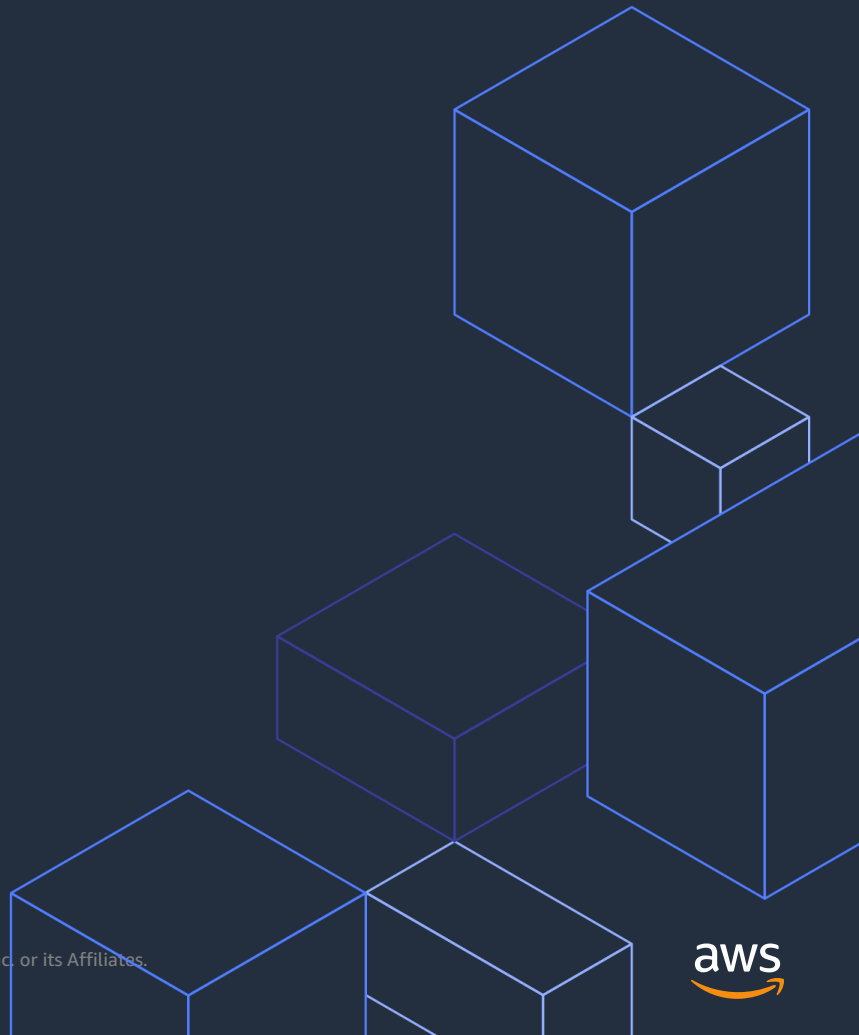
CloudWatch 面板

- 一个页面查看所有网络指标和告警
- 一个页面查看 VPN 和 Direct Connect 专线的状态
- 一个页面查看 DDoS 和网络攻击的事件

Transit Gateway 网络管理器

- 可视化覆盖各个 AWS 区域和本地站点的全球网络状况
- 查看 VPN 连接的健康状态
- 监控 TGW 的指标
- 监控网络事件

监控 API 活动



AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

监控 API 请求

CloudTrail

提供 AWS 账号的所有活动信息，包括通过管理控制台，SDK，命令行工具和其他服务的活动

CloudTrail Insights

自动从 CloudTrail 日志上分析所有管理的事件，并且检测不寻常的模式

CloudTrail

Capture

将 API 活动记录下来存为 CloudTrail 事件

Store

将事件的日志保存到安全的 S3 存储桶内，允许网络资源变更的审计。

Act

当严重的事件被检测到时，可以触发响应的行为。

例如：当一个新的 VPN 被创建了，Slack 频道将收到通知。

Review

分析在网络资源上的事件和变更。

例如：检查 Transit Gateway 路由表变化的细节

aws

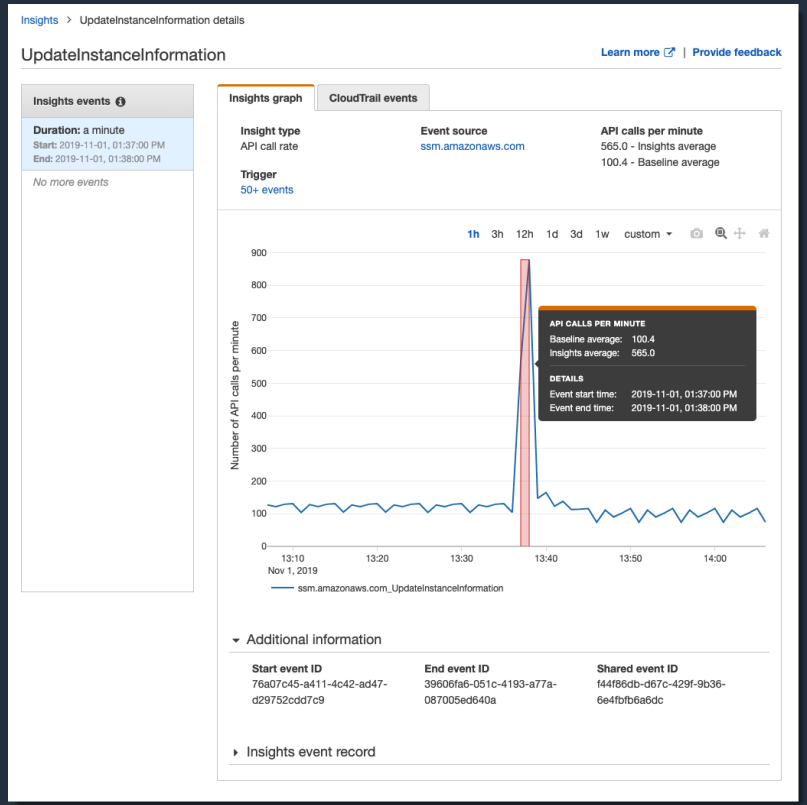
CloudTrail 日志的细节剖析

eventVersion	1.05
userIdentity	*IAM principal of the requestor*
eventTime	2020-04-15T18:41:55Z
eventSource	ec2.amazonaws.com
eventName	CreateVpnConnection
awsRegion	us-west-2
sourceIPAddress	172.16.254.34
userAgent	console.ec2.amazonaws.com
requestParameters	*Details of the request being made*
responseElements	*Result: the data requested or a success message*
requestID	171ee2e5-e23e-4e8d-86c3-4caf2d203da4
eventID	a6dcc131-30b4-4056-88a2-6b15a385d658
eventType	AwsApiCall
recipientAccountId	379063898357

aws

使用 CloudTrail Insights 进行自动的 API 请求分析

- 分析你的 CloudTrail 日志内的事件，建立一个基准线
- 当检测到不寻常的模式时，会创建一个 Insights 事件
  - 例子：当一个对第三方防火墙做变更的脚本导致 EC2 实例产生故障



如何配置 CloudTrail 和 CloudTrail Insights

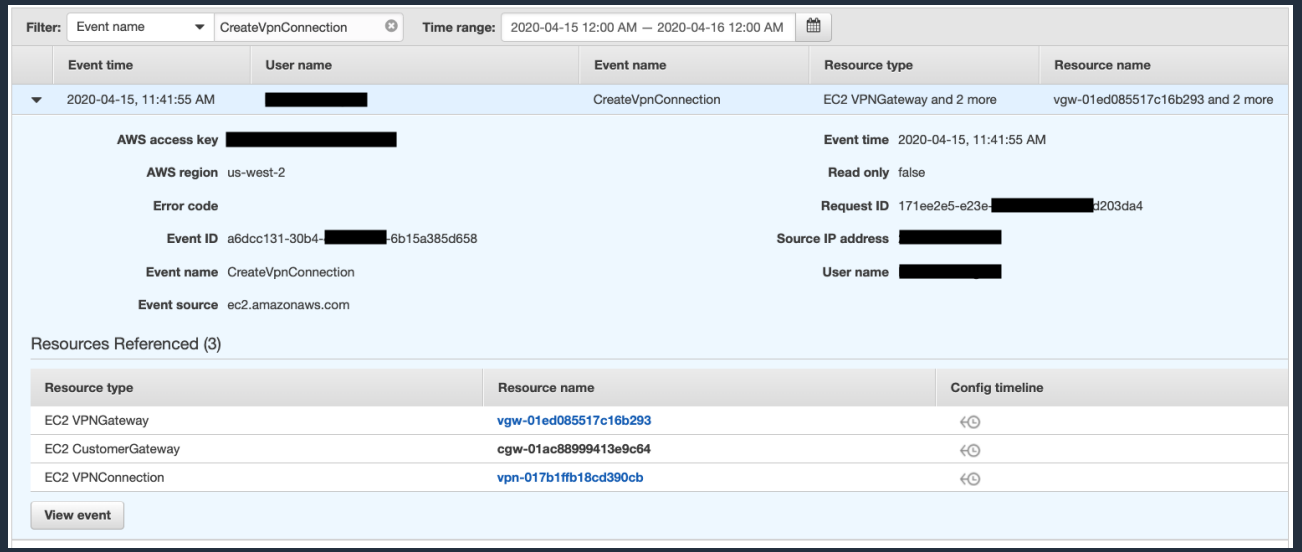
你可以创建一个 CloudTrail trial，选择你需要记录的 API 请求的类型。CloudTrail 一旦配置成功，整个账号都会生效。

要创建一个新的trail，你需要确定

- 哪一个区域需要被记录
- 对于那些读/写的 API 事件，需要选择是 log All，只读，只写还是 None
- 选择你是否要启用 *Insights* 功能
- 选择一个 S3 的存储桶来存放日志数据

如何在 CloudTrail 事件历史中进行搜索

- 选择一个*过滤类型*：比如事件名称或者资源类型
- 选择一个事件范围
- 点击查看事件来查看事件的详情（JSON格式）



CloudTrail 和 CloudTrail Insights 使用场景

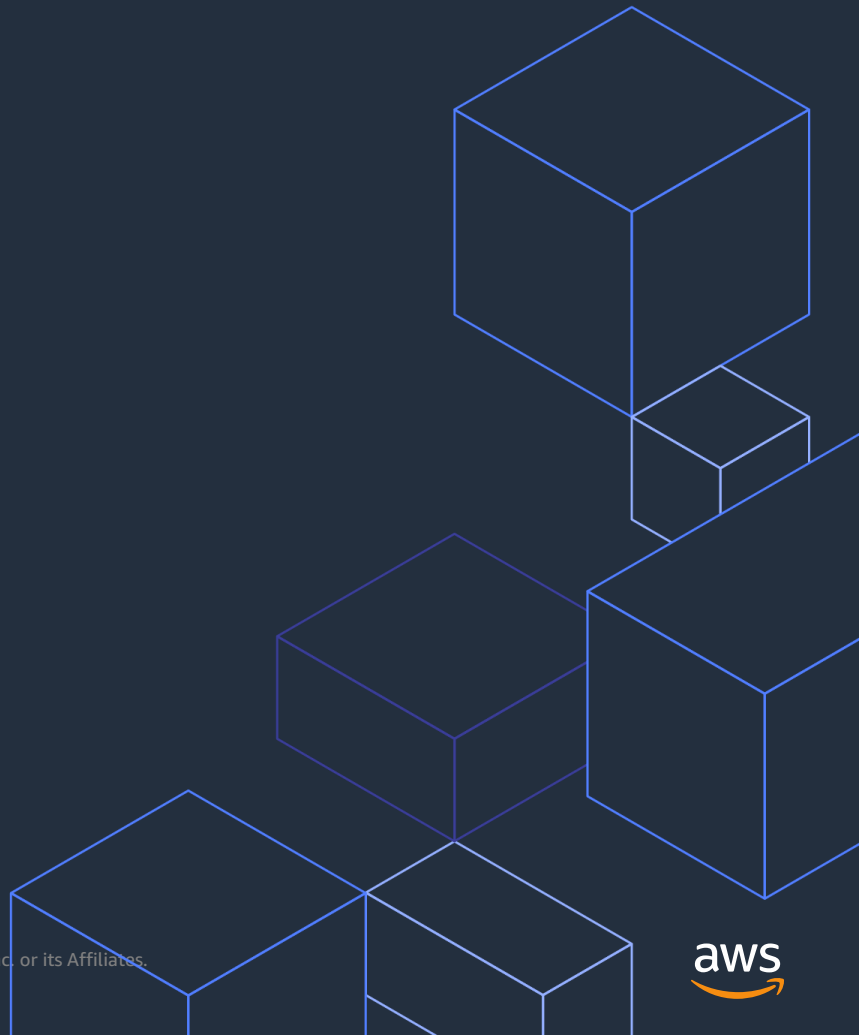
CloudTrail

- 记录网络资源的变更，比如 VPN，TGW 和 NLB
- 合规性，运维和风险审计

CloudTrail Insights

- 检测内网 IAM 权限请求的波峰
- 检测第三方软路由创建的 EC2 的峰值

Thank you!



AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营