트래픽 유형

활성화된 경우, 트래픽이 규칙에 도달할 때마다 트래픽 로그가 생성됩니다. 이러한 로그 상호 작용은 소스 및 대상 IP 주소, 포트 번호 및 사용된 프로토콜을 포함하여 수신 및 발신 트래픽에 대한 정보를 기록합니다. 로그는 활동을 모니터링하거나, 잠재적인 보안 침해를 조사하거나, 방화벽의 상태를 계속 감시하는 네트워크 감사에 매우 유용합니다. 트래픽 가시성은 언제든지 활성화할 수 있지만 클라우드 서비스 제공자 계정을 온보딩하고 게이트웨이 정책을 할당한 직후에는 트래픽을 활성화하는 것이 좋습니다.

트래픽 가시성을 활성화하는 것은 클라우드 계정 유형마다 다른 프로세스이지만, 일반적으로 클라우드 계정의 지역, 모니터링할 VPC/VNet, 네트워크 보안 그룹 및 로그용 클라우드 스토리지 계정과 같은 계정 특성을 식별해야 합니다.

쉬운 설정 마법사를 사용하여 계정을 온보딩하지 않은 경우 또는 Easy Setup wizard(쉬운 설정 마법사)에서 트래픽 가시성을 활성화하지 않은 경우에는 다음 로그를 활성화하는 것이 좋습니다.

- NSG 플로우 로그
- VPC 플로우 로그
- DNS 로그
- Route53 쿼리 로깅

- DNS 로그 활성화, 1 페이지
- VPC 플로우 로그 활성화, 3 페이지

DNS 로그 활성화

AWS: DNS 로그 활성화

이전 섹션의 CloudFormation 템플릿에서 스택을 생성하는 동안 S3 버킷이 생성된 경우, route53 쿼리 로그의 대상 역할을 하는 템플릿에 의해 S3 버킷이 생성됩니다. DNS 쿼리 로그에 대해 모니터링되는 VPC는 수동으로 추가해야 합니다.

단계 **1** AWS 콘솔에서 Route53Query Logging(Route53Query 로깅)을 클릭합니다.

단계 **2** 템플릿으로 생성된 쿼리 로거를 선택합니다. 템플릿에 제공된 접두사 이름을 가진 로거를 찾습니다.

단계 **3** 선택 및 트래픽 인사이트를 가져올 모든 VPC를 선택하고 **Add(**추가**)**를 클릭합니다.

1. "쿼리를 로깅하는 VPC" 섹션에서 **Log querys for VPCs(VPC**에 대한 쿼리 로깅**)** 또는 **Add VPC(VPC** 추가**)**를 클릭합니다.
2. 모든 VPC를 선택하고 **Choose(**선택**)**를 클릭합니다.

GCP: DNS 로그 활성화

GCP DNS 쿼리 로그를 활성화하려면 아래 단계를 수행합니다.

단계 **1** GCP 콘솔에서 VPC 네트워크로 이동합니다.

단계 **2** Google Cloud 쉘을 열고 다음 명령을 실행합니다.

```
gcloud dns policies create POLICY_NAME --networks=NETWORK --enable-logging
```

단계 **3** **Cloud Storage(**클라우드 스토리지**)** 섹션으로 이동하여 스토리지 버킷을 생성합니다. 스토리지 버킷을 생성할 때 모든 항목을 기본값으로 둘 수 있습니다.

Note *DNS* 및 *VPC* 로그 모두 동일한 클라우드 스토리지 버킷을 공유할 수 있습니다.

단계 **4** **Logs Route(**로그 경로**)** 섹션으로 이동합니다.

단계 **5** **Create Sink(**싱크 생성**)**를 클릭합니다.

단계 **6** 싱크 이름을 제공합니다.

단계 **7** 싱크 서비스에 대해 "클라우드 스토리지 버킷"을 선택합니다.

단계 **8** 위에서 생성한 클라우드 스토리지 버킷을 선택합니다.

단계 **9** "Choose logs to include in sink(싱크에 포함할 로그 선택)" 섹션에서 `resource.type="dns_query"` 문자열을 입력합니다.

아래 단계는 GCP에 대한 VPC 플로우 로그의 단계와 동일합니다. 클라우드 스토리지 버킷을 공유하는 경우 아래 단계를 한 번만 수행하면 됩니다.

단계 **10** **Create Sink(**싱크 생성**)**를 클릭합니다.

단계 **11** **IAM** > **Roles(**역할**)**로 이동합니다.

단계 **12** **storage.buckets.list** 권한이 있는 사용자 지정 역할을 생성합니다.

단계 **13** 다음 권한으로 다른 사용자 지정 역할을 생성합니다.

storage.buckets.get storage.objects.get storage.objects.list.

단계 **14** 두 사용자 지정 역할을 모두 멀티 클라우드 방어 컨트롤러에 대해 생성된 서비스 계정에 추가합니다. 두 번째 사용자 지정 역할을 추가할 때 다음 조건을 입력합니다.

```
(resource.type == "storage.googleapis.com/Bucket" || resource.type ==
 "storage.googleapis.com/Object") &&
resource.name.startsWith('projects/_/buckets/<cloud storage name>')
```

단계 **15** **Pub/Subs**로 이동합니다.

단계 **16** **Create Topic(**주제 생성**)**을 클릭합니다.

단계 **17** 주제 이름을 제공하고 **create(**생성**)**를 클릭합니다.

단계 **18** **Subscriptions(**구독**)**를 클릭합니다. 방금 생성한 주제에 대해 생성된 구독이 있음을 확인할 수 있습니다.

단계 **19** 구독을 편집합니다.

단계 **20** 전달 유형을 **Push(**푸시**)**로 변경합니다.

단계 **21** **Push(**푸시**)**를 선택하면 엔드포인트 URL을 입력합니다.

`https://prod1-webhook.vtxsecurityservices.com:8093/webhook/<tenant name> /gcp/cloudstorage.sys`. 테넌트 이름은 멀티 클라우드 방어에 의해 할당됩니다. 테넌트 이름을 보려면 멀티 클라우드 방어 컨트롤러(으)로 이동하고 사용자 이름을 클릭합니다.

단계 **22** **Update(**업데이트**)**를 클릭합니다.

단계 **23** Google Cloud 쉘을 열고 클라우드 스토리지 알림을 생성하고 `gsutil notification create -t <TOPIC_NAME\> -f json gs://<BUCKET_NAME>` 명령을 실행합니다.

Azure: DNS 로그

Azure는 현재 DNS 로그 쿼리를 표시하지 않습니다. 멀티 클라우드 방어 컨트롤러은(는) 이 클라우드 서비스 제공자의 로그를 활성화할 수 없습니다.

VPC 플로우 로그 활성화

AWS: VPC 플로우 로그 활성화

이전 섹션의 CloudFormation 템플릿에서 스택을 생성하는 동안 S3 버킷이 생성된 경우, VPC 플로우 로그의 대상 역할을 하는 템플릿에 의해 S3 버킷이 생성됩니다. 각 VPC에 대해 플로우 로그를 활성화해야 합니다.

AWS VPC 흐름 로그를 활성화하려면 아래 단계를 수행합니다.

단계 **1** AWS 콘솔에서 VPC 섹션으로 이동합니다.

단계 **2** VPC를 선택하고 해당 VPC에 대한 **Flow Logs(**플로우 로그**)** 탭을 선택합니다.

단계 **3** 필터로 **All(**모두**)**을 선택합니다.

단계 **4** 대상으로 **Send to an Amazon S3 bucket(Amazon S3** 버킷으로 보내기**)**를 선택합니다.

단계 **5** CloudFormation 템플릿 스택의 tutput에서 복사한 S3 버킷 ARN을 제공합니다.

단계 **6** 로그 기록 형식으로 **Custom Format(**사용자 지정 형식**)**을 선택합니다.

단계 **7** 로그 형식 드롭다운에서 모든 필드를 선택합니다.

단계 **8** **Create Flow Log(**플로우 로그 생성**)**를 클릭합니다.

GCP: VPC 플로우 로그 활성화

GCP VPC 흐름 로그를 활성화하려면 아래 단계를 수행합니다.

단계 **1** GCP 콘솔에서**VPC network(VPC** 네트워크**)**로 이동합니다.

단계 **2** VPC 흐름 로그를 활성화하려면 **subnet(**서브넷**)**을 선택합니다.

단계 **3** 플로우 로그가 **On(**켜짐**)**으로 설정되어 있는지 확인합니다. 꺼져 있는 경우 **Edit(**편집**)** 옵션을 클릭하고 플로우 로그를 켭니다.

단계 **4** 플로우 로그를 활성화할 모든 서브넷에서 플로우 로그를 켭니다.

단계 **5** **Cloud Storage(**클라우드 스토리지**)** 섹션으로 이동하여 스토리지 버킷을 생성합니다. 스토리지 버킷을 생성할 때 모든 항목을 기본값으로 둘 수 있습니다.

Note DNS 및 VPC 로그 모두 동일한 클라우드 스토리지 버킷을 공유할 수 있습니다.

단계 **6** **Logs Route(**로그 경로**)** 섹션으로 이동합니다.

단계 **7** **Create Sink(**싱크 생성**)**를 클릭합니다.

단계 **8** 싱크의 이름을 입력합니다.

단계 **9** 싱크 서비스용 **Cloud Storage bucket(**클라우드 스토리지 버킷**)**을 선택합니다.

단계 **10** 위에서 생성한 클라우드 스토리지 버킷을 선택합니다.

단계 **11** **Choose logs to include inink(**싱크에 포함할 로그 선택**)** 섹션에 `logName:(projects/<project-id>/logs/compute.googleapis.com%2Fvpc_flows)` 문자열을 입력합니다.

클라우드 스토리지 버킷을 공유하는 경우 이 절차의 남은 단계를 한 번만 수행하면 됩니다.

단계 **12** **Create Sink(**싱크 생성**)**를 클릭합니다.

단계 **13** **IAM** > **Roles(**역할**)**로 이동합니다.

단계 **14** `storage.buckets.list` 권한이 있는 사용자 지정 역할을 하나 생성합니다.

단계 **15** 다음 권한이 있는 맞춤형 역할을 하나 생성합니다. `storage.buckets.get storage.objects.get storage.objects.list`.

단계 **16** 두 사용자 지정 역할을 모두 멀티 클라우드 방어 컨트롤러에 대해 생성된 서비스 계정에 추가합니다. 두 번째 사용자 지정 역할을 추가할 경우 다음 조건을 입력합니다.

```
(resource.type == "storage.googleapis.com/Bucket" || resource.type ==
"storage.googleapis.com/Object") && resource.name.startsWith('projects/_/buckets/<cloud
storage name>')
```

단계 **17** **Pub/Subs**로 이동합니다.

단계 **18** **Create Topic(**주제 생성**)**을 클릭합니다.

단계 **19** 주제 이름을 제공하고 **Create(**생성**)**를 클릭합니다.

단계 **20** **Subscriptions(**구독**)**를 클릭합니다. 18단계에서 생성한 주제에 대한 구독이 생성됩니다.

단계 **21** 구독을 편집합니다.

단계 **22** **Delivery(**전달**)** 유형을 **Push(**푸시**)**로 변경합니다.

단계 **23** 이 URL을 엔드포인트 URL로 입력합니다. `https://prod1-webhook.vtxsecurityservices.com:8093/webhook/<tenant name> /gcp/cloudstorage.sys`.

멀티 클라우드 방어은(는) 테넌트 이름을 자동으로 할당합니다. 테넌트 이름을 보려면 멀티 클라우드 방어 컨트롤러(으)로 이동하고 사용자 이름을 클릭합니다.

단계 **24** **Update(**업데이트**)**를 클릭합니다.

단계 **25** Google Cloud 쉘을 열고 `gsutil notification create -t <TOPIC_NAME> -f json gs://<BUCKET_NAME>` 명령을 실행합니다.

Azure: NSG 플로우 로그 활성화

Azure VPC 흐름 로그를 활성화하려면 아래 단계를 수행합니다.

단계 **1** Azure 포털에서 **Resource Groups(**리소스 그룹**)** 섹션으로 이동합니다.

단계 **2** **Create(**생성**)** 버튼을 클릭합니다.

단계 **3** 구독을 선택하고 이 새 리소스 그룹의 이름을 제공합니다.

단계 **4** **Region(**지역**)**을 선택합니다. (예: (US) 미국동부).

단계 **5** **Review + create(**검토 + 생성**)** 버튼을 클릭합니다.

단계 **6** 스토리지 계정 섹션으로 이동하여 **Create(**생성**)** 버튼을 클릭합니다.

단계 **7** 방금 생성한 **Subscription(**구독**)** 및 **Resource(**리소스**)** 그룹을 선택합니다.

단계 **8** 리소스 그룹으로 동일한 **region(**지역**)**을 선택합니다.

단계 **9** 스토리지 계정의 이름을 제공합니다.

이중화는 LRS(Local-redundancy storage)를 사용할 수 없습니다.

단계 **10** **Review + create(**검토 + 생성**)** 버튼을 클릭합니다. NSG 플로우 로그가 저장되는 스토리지 계정이 생성됩니다.

단계 **11** **Subscription(**구독**)** 섹션으로 이동하여 최근에 생성된 구독을 찾습니다.

단계 **12** **Resource Providers(**리소스 제공자**)**로 이동합니다.

단계 **13** `microsoft.insights` 및 `Microsoft.EventGrid` 제공자가 등록되었는지 확인합니다. 등록되지 않은 경우 **Register(**등록**)** 버튼을 클릭합니다.

단계 **14** **Network Watcher(**네트워크 감시자**)** 섹션으로 이동합니다.

단계 **15** **Add(**추가**)**를 클릭하고 NSG 플로우 로그를 활성화할 지역을 추가합니다.

단계 **16** **Network Watcher(**네트워크 감시자**)** > **NSG flow logs(NSG** 플로우 로그**)**로 이동합니다.

단계 **17** NSG 플로우 로그를 활성화할 NSG에 대한 플로우 로그를 생성합니다. 위에서 생성한 스토리지 계정을 제공합니다. **Retention days(**보존 일수**)**를 30으로 설정합니다.

단계 **18** 생성된 스토리지 계정으로 이동하여 **Events(**이벤트**)**를 클릭합니다.

단계 **19** **Event Subscription(**이벤트 구독**)**을 클릭합니다.

단계 **20** 이 이벤트 구독의 이름을 제공합니다.

단계 **21** 위에서 생성한 리소스 그룹을 선택합니다.

단계 **22** 시스템 항목 이름을 제공합니다.

단계 **23** **Filter to Event Types(**이벤트 유형 필터링**)**의 경우 기본값은 **Blob Created(**블롭 생성됨**)** 및 **Blob Deleted(**블롭 삭제됨**)**입니다.

단계 **24** **Endpoint Type(**엔드포인트 유형**)**에 대해 **Webhook**를 선택합니다.

단계 **25** **Select endpoint(**엔드포인트 선택**)** 링크를 클릭합니다.

구독자 엔드포인트는 `https://prod1- webhook.vtxsecurityservices.com:8093/webhook/<tenant_name>/azure`입니다. 테넌트 이름은 멀티 클라우드 방어에 의해 할당됩니다. 멀티 클라우드 방어 컨트롤러에서 사용자 이름을 클릭하여 테넌트 이름을 찾을 수 있습니다.