Types of Traffic

When enabled, traffic logs are generated whenever traffic hits a rule. These log interactions record information about incoming and outgoing traffic, including the source and destination IP addresses, port numbers, and protocols used. Logs can be incredibly useful to audit the network; monitor activity, investigate potential security breaches, or simply keep an eye on what is happening with your firewall. Traffic visibility can be enabled at any time but we strongly recommend enabling traffic immediately after onboarding a cloud service provider account and assigning a gateway policy.

Enabling traffic visibility is a different process for every cloud account type, but typically you will need to identify account characteristics such as your cloud account's region, VPC/VNet that you want to monitor, network security groups, and a cloud storage account for logs.

If you did not onboard an account with the Easy Setup wizard or if you did not enable traffic visibliilty from the Easy Setup wizard, we strongly recommend enabling the following logs:

- NSG Flow Logs
- VPC Flow Logs
- DNS Logs
- Route53 Query Logging.

Note You can download logs for flows and events. In the Time Range section, select a time range and click the download icon. A maximum of 10,000 records are downloaded in a single instance. You will need to repeat the step to download larger sets of records.

- Enable DNS Logs, on page 2
- Enable VPC Flow Logs, on page 3

Enable DNS Logs

AWS: Enable DNS Logs

If you provided a S3 bucket during the stack creation from the CloudFormation template in the previous section, a S3 bucket is created by the template that acts as the destination for the route53 Query Logs. The VPCs that are monitored for the DNS query logs must be added manually.

Procedure

Step 1 In AWS Console go to the Route53Query Logging .

Step 2 Select the **Query Logger** created by the template. Locate the logger with the prefix name provided in the template.

Step 3 Select and all the VPCs for which you want to get the traffic insights and clikc **Add**.

a. Under the " VPCs that queries are logged for" section, click **Log queries for VPCs** or **Add VPC**.

b. Select all the VPCs and click **Choose**.

GCP: Enable DNS Logs

To enable GCP DNS query logs, follow the below steps.

Procedure

Step 1 Navigate to VPC network in GCP console.

Step 2 Open Google cloud shell and execute this command:

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

Step 3 Navigate to **Cloud Storage** section and create a storage bucket. You can leave everything as default when creating storage bucket.

Note *Both DNS and VPC logs can share the same cloud storage bucket.*

Step 4 Navigate to **Logs Route** section.

Step 5 Click on **Create Sink**.

Step 6 Provide a sink name.

Step 7 Select "Cloud Storage bucket" for sink service.

Step 8 Select the cloud storage bucket that was created above.

Step 9 In "Choose logs to include in sink" section, put in this string: `resource.type="dns_query"`.

Below steps are the same as mentioned in VPC flow log for GCP. If you are sharing cloud storage bucket, you only need to perform below steps once.

Step 10 Click **Create Sink**.

Step 11 Navigate to **IAM** > **Roles**.

Step 12 Create a custom role with this permission: **storage.buckets.list**.

Step 13 Create another custom role with following permission:

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

Step 14 Add both custom role to the service account created for Multicloud Defense Controller. When adding the second custom role, put this condition:

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

Step 15 Navigate to **Pub/Subs**.

Step 16 Click on **Create Topic**.

Step 17 Provide a Topic name and click **create**.

Step 18 Click on **Subscriptions**. You will find that there is a subscription created for the topic that was just created.

Step 19 Edit the subscription.

Step 20 Change Delivery type as **Push**.

Step 21 Once **Push** is selected, enter in the endpoint URL: `https://prod1-webhook.vtxsecurityservices.com:8093/webhook/<tenant name>/gcp/cloudstorage`. Tenant name is assigned by Multicloud Defense. To view tenant name, navigate to Multicloud Defense Controller and click on your username.

Step 22 Click **Update**.

Step 23 Create a cloud storage notification by opening a Google cloud shell and execute this command: `gsutil notification create -t <TOPIC_NAME\> -f json gs://<BUCKET_NAME>`.

Azure: DNS Logs

Azure currently does not expose DNS log queries. Multicloud Defense Controller cannot enable logs for this cloud service provider.

Enable VPC Flow Logs

AWS: Enable VPC Flow Logs

If you provided a S3 bucket during the stack creation from the CloudFormation template in the previous section, a S3 bucket is created by the template that acts as the destination for the VPC flow logs. Flow logs must be enabled for each of the VPCs.

To enable AWS VPC flow logs, follow the below steps:

Procedure

Step 1 In the AWS Console, go to the VPCs section.
Step 2 Select the VPC and select the **Flow Logs** tab for that VPC.
Step 3 Select **All** as the filter.
Step 4 Select **Send to an Amazon S3 bucket** as the destination.
Step 5 Provide the S3 bucket ARN copied from the tutputs of the CloudFormation template stack.
Step 6 Choose **Custom Format** as the log record format.
Step 7 Select all the fields from the log format dropdown.
Step 8 Click **Create Flow Log**.

GCP: Enable VPC Flow Logs

To enable GCP VPC flow logs, follow the below steps.

Procedure

Step 1 In the GCP console, navigate to **VPC network**
Step 2 to enable the VPC flow log, select the **subnet**.
Step 3 Ensure that flow logs is turned **On**. If it is off, click the **Edit**option and turn flow logs on.
Step 4 Turn on flow log on all subnets where you want to enable flow log.
Step 5 Navigate to **Cloud Storage** section and create a storage bucket. You can leave everything as default when creating storage bucket.

Note Both DNS and VPC logs can share the same cloud storage bucket.

Step 6 Navigate to the **Logs Route** section.
Step 7 Click **Create Sink**.
Step 8 Enter a name for the sink.
Step 9 Select **Cloud Storage bucket** for sink service.
Step 10 Select the cloud storage bucket that was created above.
Step 11 In the **Choose logs to include in sink** section, enter this string: `logName:(projects/<project-id>/logs/compute.googleapis.com%2Fvpc_flows)`

If you are sharing cloud storage bucket, you only need to perform the remaning steps of this procedure once.

Step 12 Click **Create Sink**.
Step 13 Navigate to **IAM** > **Roles**.
Step 14 Create one custom role with this permission: `storage.buckets.list`.
Step 15 Create one custom role with following permission: `storage.buckets.get storage.objects.get storage.objects.list`.

Step 16 Add both custom roles to the service account created for Multicloud Defense Controller. When adding the second custom role, enter the following condition:

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

Step 17 Navigate to **Pub/Subs**.

Step 18 Click **Create Topic**.

Step 19 Provide a **Topic** name and click **Create**.

Step 20 Click **Subscriptions**. A subscription is created for the topic created in step 18.

Step 21 **Edit** the subscription.

Step 22 Change the **Delivery** type to **Push**.

Step 23 Enter this as the endpoint URL:`https://prod1- webhook.vtxsecurityservices.com:8093/webhook/<tenant name>/gcp/cloudstorage`.

Multicloud Defense autmoatically assigns the tenant name. To see tenant name, navigate to Multicloud Defense Controller and click on your username.

Step 24 Click **Update**.

Step 25 Open a Google cloud shell and execute the following command: `gsutil notification create -t <TOPIC_NAME> -f json gs://<BUCKET_NAME>`.

Azure: Enable NSG Flow Logs

To enable Azure VPC flow logs, follow the below steps.

Procedure

Step 1 Go to the **Resource Groups** section in Azure portal.

Step 2 Click the **Create** button.

Step 3 Select the subscription and provide a name for this new resource group.

Step 4 Select a **Region**. (example: (US) East US).

Step 5 Click the **Review + create** button.

Step 6 Go to the **storage accounts** section and click the **Create** button.

Step 7 Select the **Subscription** and **Resource** group that was just created.

Step 8 Select the same **region** as the resource group.

Step 9 Provide a name for the storage account.

Note that **Redundancy cannot** be locally-redundant storage(LRS)

Step 10 Click the **Review + create** button. This creates a storage account where NSG flow logs are stored.

Step 11 Go to the **Subscription** section and find the subscription that was recently created.

Step 12 Navigate to **Resource Providers**.

Step 13 Ensure that the `microsoft.insights` and `Microsoft.EventGrid` providers are registered. If they are not registered, click the **Register** button.

Step 14 Go to the **Network Watcher** section.

Step 15 Click **Add** and add the regions that you want NSG flow logs to be enabled for.

Step 16 Go to **Network Watcher** > **NSG flow logs**.

Step 17 Create flow logs for the NSG where you want to enable NSG flow log. Provide the storage account created above. Set the **Retention days** as 30.

Step 18 Navigate to the storage account created and click on **Events**.

Step 19 Click **Event Subscription**.

Step 20 Provide a name for this event subscription.

Step 21 Select the resource group that was created above.

Step 22 Provide a **System Topic Name**.

Step 23 For **Filter to Event Types**, the default value is **Blob Created** and **Blob Deleted**.

Step 24 For **Endpoint Type**, select **Web Hook**.

Step 25 Click the **Select an endpoint** link.

The Subscriber Endpoint is `https://prod1-webhook.vtxsecurityservices.com:8093/webhook/<tenant_name>/azure`. Tenant name is assigned by Multicloud Defense. You can find tenant name by clicking on the username in Multicloud Defense Controller.