

# Cloud Network Monitoring Use Cases



## Expensive Network Traffic

### ✓ Cross AZ traffic

#### Cross AZ traffic

Cross availability zone (AZ) traffic in the cloud can be expensive.

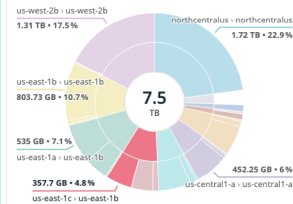
#### Top cross-AZ traffic - filtered by env variable

This pie chart shows the breakdown of traffic from any network flow with an env tag. Filtering for a specific env at the top of the dashboard will update the pie chart to show cross AZ traffic for within that env.

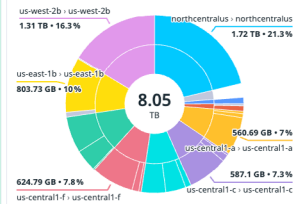
#### Top cross-AZ traffic - filtered by service variable

This pie chart shows the breakdown of traffic from any network flow with a service tag. Filtering for a specific service at the top of the dashboard will update the pie chart to show cross AZ traffic for just that service.

Top cross-AZ traffic - filtered by env variable



Top cross-AZ traffic - filtered by service variable



| CLIENT AVAILABILITY ZONE | SERVICE        | COUNT      | SHARE   |
|--------------------------|----------------|------------|---------|
| northcentralus           | northcentralus | 1,716.1 GB | 22.88 % |
| us-west-2b               | us-west-2b     | 1,310.7 GB | 17.47 % |
| us-east-1b               | us-east-1b     | 803.7 GB   | 10.71 % |
| us-east-1a               | us-east-1a     | 535.0 GB   | 7.13 %  |
| us-central-1a            | us-central-1a  | 452.3 GB   | 6.03 %  |
| us-central-1f            | us-central-1f  | 438.3 GB   | 5.84 %  |
| us-east-1c               | us-east-1c     | 405.4 GB   | 5.40 %  |
| us-east-1b               | us-east-1b     | 357.7 GB   | 4.77 %  |
| us-east-1a               | us-east-1a     | 319.4 GB   | 4.26 %  |
| us-east-1a               | us-east-1a     | 293.5 GB   | 3.91 %  |
| us-west-1b               | us-west-1b     | 90.9 GB    | 1.21 %  |
| us-central-1f            | us-central-1f  | 89.4 GB    | 1.14 %  |
| us-east-1c               | us-east-1c     | 83.6 GB    | 1.11 %  |
| us-central-1c            | us-central-1c  | 80.5 GB    | 1.07 %  |

## About Datadog

Datadog is a leading SaaS-based observability and security platform that brings together telemetry from across your tech environment—including infrastructure metrics, application traces, and logs—together in a single platform. Our monitoring capabilities include customizable alerting and monitoring reports and visualization tools like out-of-the-box dashboards, making it easy and fast to investigate and resolve issues. With integrations with major cloud providers and network vendors, Datadog provides end-to-end network visibility in a single pane of glass. Explore key Cloud Network Monitoring metrics that provide insights into real-world use cases.

### 1. CROSS AZ TRAFFIC

Cross availability zone (AZ) traffic in the cloud could be expensive. This section provides you with an overview of how to view expensive AZ traffic by env or service.

| QUERY DESCRIPTION                                   | QUERY                                  | GROUP BY - CLIENT | GROUP BY - SERVER | MEASURE                            |
|---|--|-------------------|-------------------|------------------------------------|
| Top cross-AZ traffic - filtered by env variable     | (client_env:* OR server_env:*)         | availability-zone | availability-zone | sum of (Bytes Sent) limit to (100) |
| Top cross-AZ traffic - filtered by service variable | (client_service:* OR server_service:*) | availability-zone | availability-zone | sum of (Bytes Sent) limit to (100) |

### 2. EXTERNAL TRAFFIC

External traffic in the cloud could be expensive. This section provides you with an overview of top external domains that the service is sending traffic to and how much traffic.

| QUERY DESCRIPTION                  | QUERY   | GROUP BY - CLIENT | GROUP BY - SERVER | MEASURE                            |
|------------------------------------|---|-------------------|-------------------|------------------------------------|
| External network traffic by domain | client_service:* network.server.ip_type:other -server_domain:*datadoghq.com | ungrouped traffic | domain            | sum of (Bytes Sent) limit to (100) |

### 3. TRAFFIC THROUGH GATEWAYS

Traffic going through NAT gateways, Transit gateways, or Internet gateways could be expensive. This section provides you with an overview of top traffic by host going through NAT, Transit, and Internet gateways.

| QUERY DESCRIPTION                    | QUERY   | GROUP BY - CLIENT | GROUP BY - SERVER | MEASURE                            |
|--------------------------------------|---|-------------------|-------------------|------------------------------------|
| Top host to NAT gateway traffic      | network.server.ip_type:other server_gateway_type:aws_nat_gateway      | host              | gateway_id        | sum of (Bytes Sent) limit to (100) |
| Top host to internet gateway traffic | network.server.ip_type:other server_gateway_type:aws_internet_gateway | host              | gateway_id        | sum of (Bytes Sent) limit to (100) |

### ✓ External traffic

#### External network traffic by domain

| DOMAIN   | ↓ BYTES SENT |
|--|--------------|
| monitoring.googleapis.com  | 577.73 GB    |
| b0c0b159866d.tr6341.northcentralus1-a.workerdatabase.windows.net | 367.23 GB    |
| api.segment.io   | 74.18 GB     |
| 6135d430-83c6-468d-a57c-788b61049ec.opinsights.azure.com         | 46.11 GB     |
| s3.us-west-2.amazonaws.com                                       | 42.29 GB     |
| cd4998cf03.tr5743.northcentralus1-a.workerdatabase.windows.net   | 34.85 GB     |
| 6052fb71-80c4-43aa-8058-e3b1258bb726.ods.opinsights.azure.com    | 32.07 GB     |

#### External network traffic

External network traffic can be another costly source of traffic. See which domains the service selected at the top of this page is talking to, and how much traffic is being sent to the respective domains.

### ✓ Traffic through gateways

#### Traffic through Gateways

Traffic going through NAT gateways, Transit gateways, or Internet gateways could be another source of expensive traffic.

This table shows your top host and gateway talkers, including NAT, Transit, and Internet gateways as well as VPC endpoints.

Top host to NAT gateway traffic

Q Search

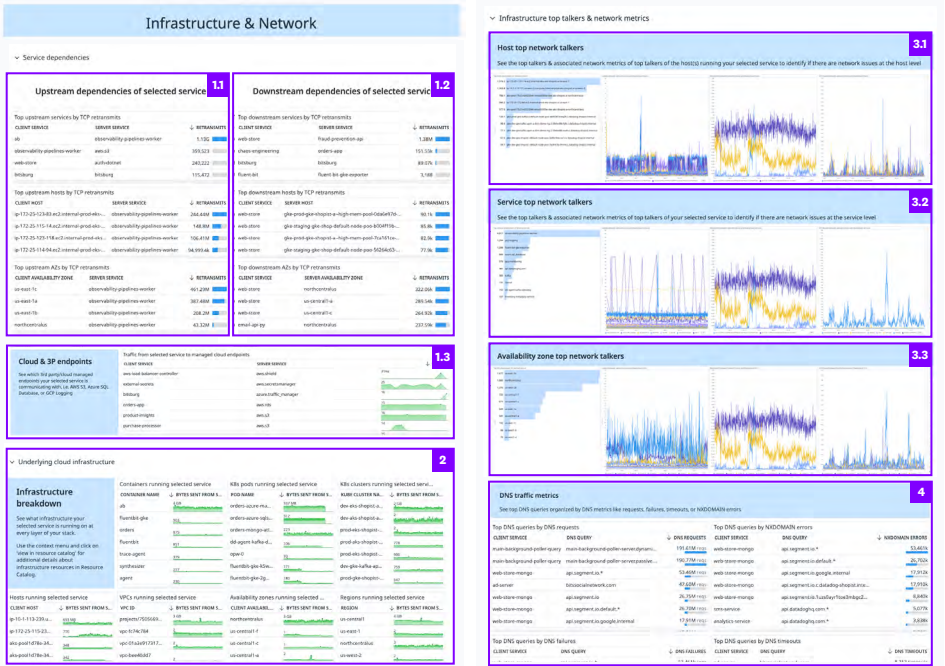
| CLIENT HOST   | GATEWAY ID             | ↓ BYTES SENT |
|---|------------------------|--------------|
| ip-172-25-117-185.ec2.internal-prod-eks-shopist-a-us-east-1 | nat-06990cc2a9472062   | 194.3 GB     |
| ip-172-25-123-83.ec2.internal-prod-eks-shopist-a-us-east-1  | nat-06aff2320e85d2fed  | 144.0 GB     |
| ip-172-25-115-14.ec2.internal-prod-eks-shopist-a-us-east-1  | nat-052037aef65216d93  | 116.1 GB     |
| ip-172-25-114-94.ec2.internal-prod-eks-shopist-a-us-east-1  | nat-052037aef65216d93  | 113.3 GB     |
| ip-172-25-123-118.ec2.internal-prod-eks-shopist-a-us-east-1 | nat-06aff2320e85d2fed  | 93.5 GB      |
| ip-172-25-118-88.ec2.internal-prod-eks-shopist-a-us-east-1  | nat-0b930cc2a5472df62  | 88.7 GB      |
| ip-172-25-120-240.ec2.internal-prod-eks-shopist-a-us-east-1 | nat-06aff2320e85d2fed  | 88.3 GB      |
| ip-172-25-117-49.ec2.internal-prod-eks-shopist-a-us-east-1  | nat-0b930cc2a5472df62  | 83.7 GB      |
| ip-172-25-118-246.ec2.internal-prod-eks-shopist-a-us-east-1 | nat-0b930cc2a5472df62  | 83.2 GB      |
| ip-173-76-173-131.ap3.internal-centralus1-a-us-east-1       | nat-06c4993730a8c476d4 | 49.4 GB      |

#### Top host to Internet gateway traffic

Q Search

| CLIENT HOST   | GATEWAY ID            | ↓ BYTES SENT |
|---|-----------------------|--------------|
| ip-10-1-113-70.us-west-2.compute.internal-prod-eks-shopist-a-us-west-2  | igw-02efd5e9b5f871ebd | 195 GB       |
| ip-10-1-112-231.us-west-2.compute.internal-prod-eks-shopist-a-us-west-2 | igw-02efd5e9b5f871ebd | 192 GB       |
| ip-10-1-112-232.us-west-2.compute.internal                              | igw-02efd5e9b5f871ebd | 181 GB       |

# Cloud Network Monitoring Use Cases



## 1. SERVICE DEPENDENCIES

### 1.1 Upstream dependencies of selected service

This section provides an overview of upstream infra for a given service.

| QUERY DESCRIPTION                        | QUERY   | GROUP BY - CLIENT | GROUP BY - SERVER | MEASURE                                 |
|--|---|-------------------|-------------------|---|
| Top upstream services by TCP retransmits | server_service:* (client_env:* OR server_env:*) | service           | service           | sum of (TCP Retransmits) limit to (100) |
| Top upstream hosts by TCP retransmits    | server_service:* (client_env:* OR server_env:*) | host              | service           | sum of (TCP Retransmits) limit to (100) |
| Top upstream AZs by TCP retransmits      | server_service:* (client_env:* OR server_env:*) | availability-zone | service           | sum of (TCP Retransmits) limit to (100) |
| Top upstream regions by TCP retransmits  | server_service:* (client_env:* OR server_env:*) | region            | service           | sum of (TCP Retransmits) limit to (100) |

### 1.2 Downstream dependencies of selected service

This section provides an overview of downstream infra for a given service.

| QUERY DESCRIPTION                          | QUERY   | GROUP BY - CLIENT | GROUP BY - SERVER | MEASURE                              |
|--|---|-------------------|-------------------|--------------------------------------|
| Top downstream services by TCP retransmits | client_service:* (client_env:* OR server_env:*) | service           | service           | sum of (TCP Refusals) limit to (100) |
| Top downstream hosts by TCP retransmits    | client_service:* (client_env:* OR server_env:*) | service           | host              | sum of (TCP Refusals) limit to (100) |
| Top downstream AZs by TCP retransmits      | client_service:* (client_env:* OR server_env:*) | service           | availability-zone | sum of (TCP Refusals) limit to (100) |
| Top downstream regions by TCP retransmits  | client_service:* (client_env:* OR server_env:*) | service           | region            | sum of (TCP Refusals) limit to (100) |

### 1.3 Traffic from selected service to managed cloud endpoints

This section provides an overview of cloud managed endpoints your selected service is communicating with.

| QUERY DESCRIPTION  | QUERY   | GROUP BY - CLIENT | GROUP BY - SERVER | MEASURE                             |
|--|---|-------------------|-------------------|-------------------------------------|
| Traffic from selected service to managed cloud endpoints | client_service:* (client_cloud_endpoint_detection:true OR server_cloud_endpoint_detection:true) | service           | service           | sum of (TCP Latency) limit to (100) |

## 2. UNDERLYING CLOUD INFRASTRUCTURE

This section shows the network performance for the underlying infrastructure of a selected service.

| QUERY DESCRIPTION                           | QUERY            | GROUP BY - CLIENT | GROUP BY - SERVER | MEASURE                            |
|---|------------------|-------------------|-------------------|------------------------------------|
| Containers running selected service         | client_service:* | container_name    | ungrouped traffic | sum of (Bytes Sent) limit to (100) |
| K8s pods running selected service           | client_service:* | pod_name          | ungrouped traffic | sum of (Bytes Sent) limit to (100) |
| K8s clusters running selected service       | client_service:* | kube_cluster_name | ungrouped traffic | sum of (Bytes Sent) limit to (100) |
| Hosts running selected service              | client_service:* | host              | ungrouped traffic | sum of (Bytes Sent) limit to (100) |
| VPCs running selected service               | client_service:* | vpc_id            | ungrouped traffic | sum of (Bytes Sent) limit to (100) |
| Availability zones running selected service | client_service:* | availability-zone | ungrouped traffic | sum of (Bytes Sent) limit to (100) |
| Regions running selected service            | client_service:* | region            | ungrouped traffic | sum of (Bytes Sent) limit to (100) |

## 3. INFRASTRUCTURE TOP TALKERS & NETWORK METRICS

### 3.1 Host top network talkers

This section provides the top talkers & associated network metrics of top talkers of the host(s) running your selected service to identify if there are network issues at the host level.

| QUERY DESCRIPTION  | QUERY            | GROUP BY - CLIENT | GROUP BY - SERVER | MEASURE                                 |
|--|------------------|-------------------|-------------------|---|
| Top hosts downstream of selected service                   | client_service:* | ungrouped traffic | host              | sum of (Bytes Sent) limit to (100)      |
| Latency between selected service and downstream hosts      | client_service:* | ungrouped traffic | host              | avg of (TCP Latency) limit to (100)     |
| Retransmits between selected service and downstream hosts  | client_service:* | ungrouped traffic | host              | sum of (TCP Retransmits) limit to (100) |
| TCP refusals between selected service and downstream hosts | client_service:* | ungrouped traffic | host              | sum of (TCP Refusals) limit to (100)    |

### 3.2 Service top network talkers

This section provides the top talkers & associated network metrics of top talkers of your selected service to identify if there are network issues at the service level.

| QUERY DESCRIPTION   | QUERY            | GROUP BY - CLIENT | GROUP BY - SERVER | MEASURE                                 |
|---|------------------|-------------------|-------------------|---|
| Top services downstream of selected service                   | client_service:* | ungrouped traffic | service           | sum of (Bytes Sent) limit to (100)      |
| Latency between selected service and downstream services      | client_service:* | ungrouped traffic | service           | avg of (TCP Latency) limit to (100)     |
| Retransmits between selected service and downstream services  | client_service:* | ungrouped traffic | service           | sum of (TCP Retransmits) limit to (100) |
| TCP refusals between selected service and downstream services | client_service:* | ungrouped traffic | service           | sum of (TCP Refusals) limit to (100)    |

### 3.3 Availability zone top network talkers

This section provides the top talkers & associated network metrics of top talkers of the availability zone(s) running your selected service to identify if there are network issues at the availability zone level.

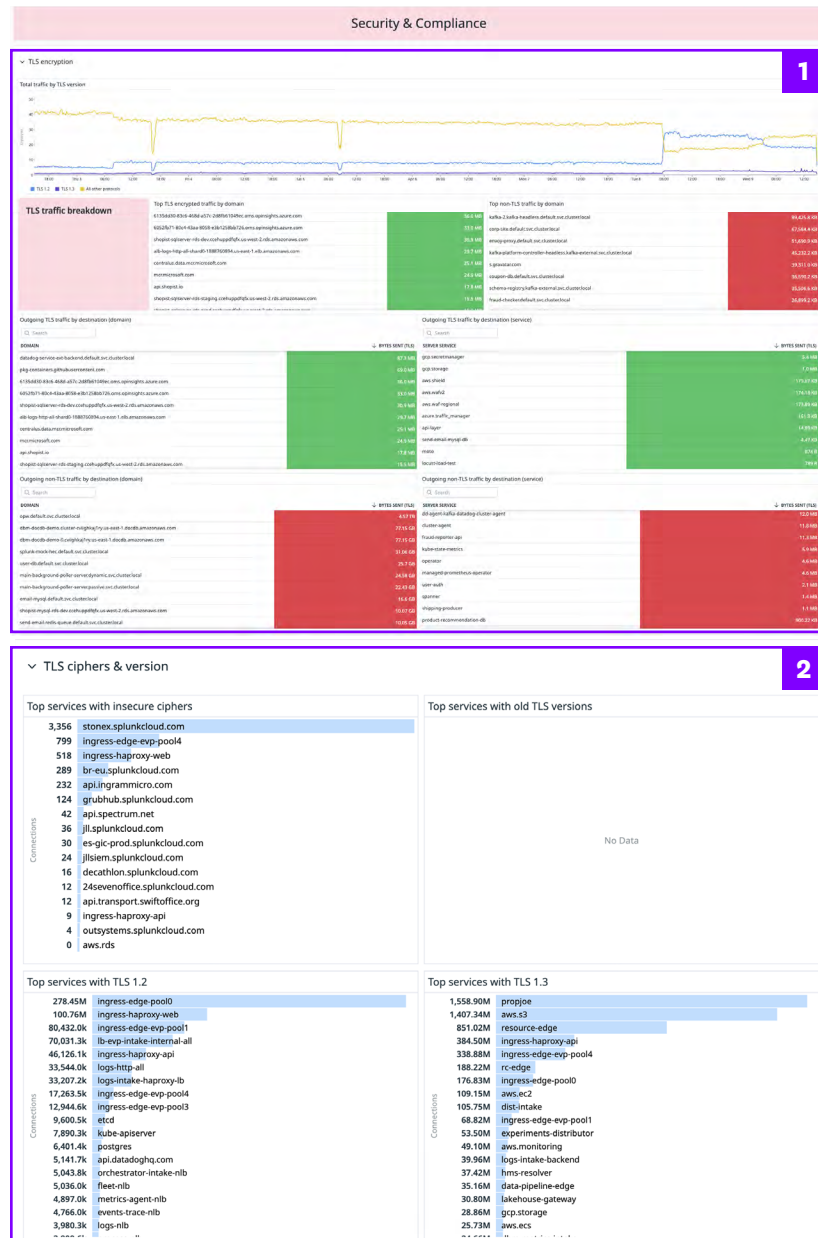
| QUERY DESCRIPTION  | QUERY            | GROUP BY - CLIENT | GROUP BY - SERVER | MEASURE                                 |
|--|------------------|-------------------|-------------------|---|
| Top AZs downstream of selected service                   | client_service:* | ungrouped traffic | availability-zone | sum of (Bytes Sent) limit to (100)      |
| Latency between selected service and downstream AZs      | client_service:* | ungrouped traffic | availability-zone | avg of (TCP Latency) limit to (100)     |
| Retransmits between selected service and downstream AZs  | client_service:* | ungrouped traffic | availability-zone | sum of (TCP Retransmits) limit to (100) |
| TCP refusals between selected service and downstream AZs | client_service:* | ungrouped traffic | availability-zone | sum of (TCP Refusals) limit to (100)    |

## 4. DNS TRAFFIC

This section provides top DNS queries by DNS metrics like requests, failures, timeouts, or NXDOMAIN errors.

| QUERY DESCRIPTION                  | QUERY            | GROUP BY - CLIENT | GROUP BY - SERVER | MEASURE                                 |
|------------------------------------|------------------|-------------------|-------------------|---|
| Top DNS queries by DNS requests    | client_service:* | service           | network.dns_query | sum of (DNS Requests) limit to (100)    |
| Top DNS queries by NXDOMAIN errors | client_service:* | service           | network.dns_query | sum of (NXDOMAIN errors) limit to (100) |
| Top DNS queries by DNS failures    | client_service:* | service           | network.dns_query | sum of (DNS Failures) limit to (100)    |
| Top DNS queries by DNS timeouts    | client_service:* | service           | network.dns_query | sum of (DNS Timeouts) limit to (100)    |

# Cloud Network Monitoring Use Cases



## 1. TLS ENCRYPTION

This section provides visibility into top encrypted and non-encrypted TLS traffic by domain and service.

| QUERY DESCRIPTION                                 | QUERY  | GROUP BY - CLIENT | GROUP BY - SERVER | MEASURE                            |
|---|--|-------------------|-------------------|------------------------------------|
| Total traffic by TLS version (version 1.2)        | tls_version:tls_1.2  | ungrouped traffic | ungrouped traffic | sum of (Bytes Sent)                |
| Total traffic by TLS version (version 1.3)        | tls_version:tls_1.3  | ungrouped traffic | ungrouped traffic | sum of (Bytes Sent)                |
| Total traffic by TLS version (all other versions) | -tls_version:tls_1.3 -tls_version:tls_1.2 tls_encrypted:true       | ungrouped traffic | ungrouped traffic | sum of (Bytes Sent)                |
| Top TLS encrypted traffic by domain               | client_service:* -server_service:datadog-agent tls_encrypted:true  | ungrouped traffic | domain            | sum of (Bytes Sent) limit to (100) |
| Top non-TLS traffic by domain                     | client_service:* -server_service:datadog-agent tls_encrypted:false | ungrouped traffic | domain            | sum of (Bytes Sent) limit to (100) |
| Outgoing TLS traffic by destination (domain)      | client_service:* -server_service:datadog-agent tls_encrypted:true  | ungrouped traffic | domain            | sum of (Bytes Sent) limit to (100) |
| Outgoing TLS traffic by destination (service)     | client_service:* -server_service:datadog-agent tls_encrypted:true  | ungrouped traffic | service           | sum of (Bytes Sent) limit to (100) |
| Outgoing non-TLS traffic by destination (domain)  | client_service:* -server_service:datadog-agent tls_encrypted:false | ungrouped traffic | domain            | sum of (Bytes Sent) limit to (100) |
| Outgoing non-TLS traffic by destination (service) | client_service:* -server_service:datadog-agent tls_encrypted:false | ungrouped traffic | service           | sum of (Bytes Sent) limit to (100) |

## 2. TLS CIPHERS & VERSION

This section provides visibility into services running non-secure TLS cipher suites and versions.

| QUERY DESCRIPTION                  | QUERY                            | GROUP BY - CLIENT | GROUP BY - SERVER | MEASURE  |
|------------------------------------|----------------------------------|-------------------|-------------------|--|
| Top services with insecure ciphers | tls_cipher_insecure:true         | ungrouped traffic | service           | sum of (TCP Established Connections) limit to (1000) |
| Top services with old TLS versions | tls_version:(tls_1.0 OR tls_1.1) | ungrouped traffic | service           | sum of (TCP Established Connections) limit to (1000) |
| Top services with TLS 1.2          | tls_version:tls_1.2              | ungrouped traffic | service           | sum of (TCP Established Connections) limit to (1000) |
| Top services with TLS 1.3          | tls_version:tls_1.3              | ungrouped traffic | service           | sum of (TCP Established Connections) limit to (1000) |

## Useful Links

- [Cloud Network Monitoring Docs](#)
- [Network Path Monitoring Blog](#)

# Datadog Cloud Network Monitoring

Unify your network view across multi-cloud, hybrid, and on-premises environments. Quickly correlate across applications, networks, devices, and infrastructure, and remediate issues effectively with intelligent insights and alerting.

**TRY DATADOG FOR FREE**

