Monitoring Network security (NSG) group flow

Network security group (NSG) flow logging is a functionality within Azure Network Watcher that enables the logging of details regarding IP traffic traversing a network security group. The flow data is transmitted to Azure Storage, allowing for access and exportation to various visualization tools, security information and event management (SIEM) systems, or intrusion detection systems (IDS) as per your requirements.It is essential to continuously monitor, manage, and understand your network to ensure its protection and optimization. Awareness of the network's current status, the identities of connected users, and their locations is crucial. Additionally, it is important to identify which ports are accessible from the internet, recognize expected network behavior, detect any anomalies, and be alert to sudden increases in traffic.

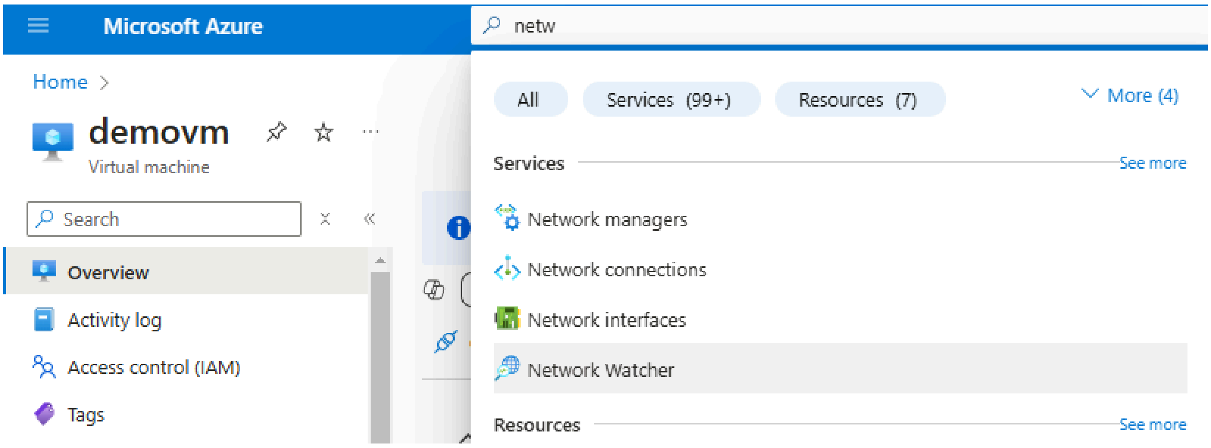
Use cases of NSG

1. **Traffic Filtering:** NSGs allow administrators to permit or deny traffic to virtual machines or subnets based on defined rules. Rules can filter traffic by source/destination IP addresses, port numbers, and protocols (TCP, UDP, or ICMP)
2. **Application Segmentation:** Use NSGs to isolate traffic between application tiers (e.g., web, application, and database) in a multi-tier architecture. Manage communication between VMs within the same subnet.
3. **Network Isolation:** Ensure workloads from different tenants or departments cannot interact by applying NSGs to subnets or network interfaces. Block unnecessary outbound traffic to prevent data exfiltration or unauthorized communication.
4. **Security Compliance:** Enforce strict network policies to comply with standards like PCI DSS, GDPR, or HIPAA. Use NSG Flow Logs to track allowed/denied traffic for security audits and forensic investigations.
5. **Secure Hybrid Connectivity:** Control traffic between on-premises networks and Azure resources connected through VPN or ExpressRoute. Apply rules to secure communication between Azure VMs in different regions or subscriptions.

The end goal of enabling Network Security Group (NSG) Flow Logs in Azure is to monitor and analyze the traffic flowing into and out of virtual machines through NSGs. This helps security engineers and administrators gain insights into allowed and denied traffic, identify potential security threats, and troubleshoot network issues. The flow logs are stored in a structured format in an Azure Storage Account and can be visualized using Traffic Analytics for advanced insights, such as traffic distribution and detection of malicious activities. This enhances security, ensures compliance, and provides actionable intelligence for network optimization.

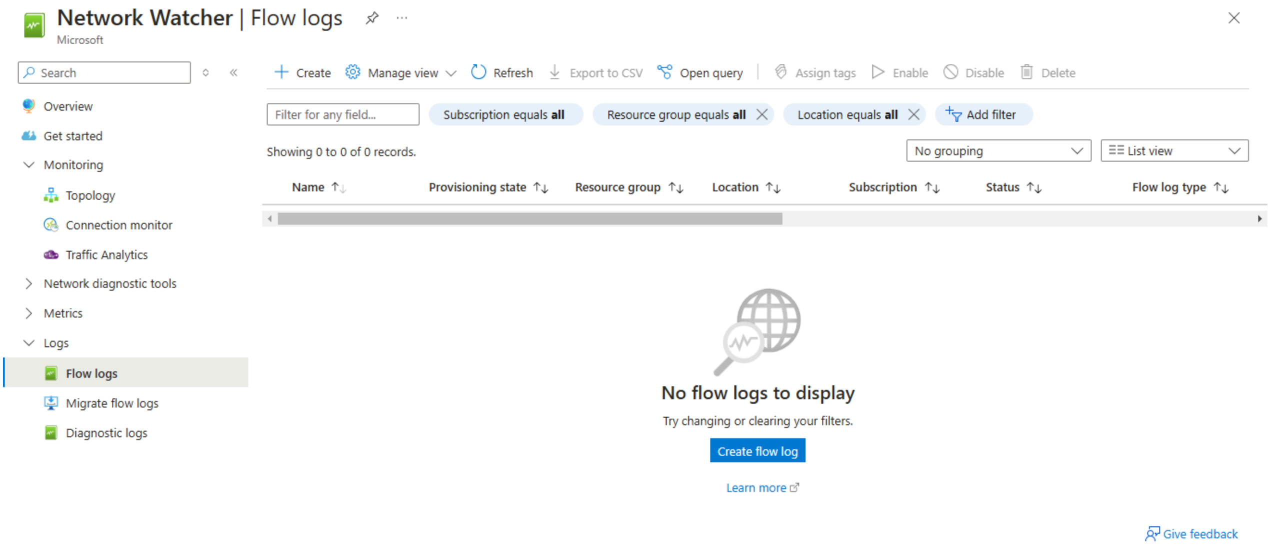
To begin with the lab

1. It is essential to attach a Network Security Group (NSG) to either the virtual machine or its corresponding subnet. Additionally, prepare an Azure Storage Account for the purpose of storing flow logs.
2. Access the Azure Portal and search for Network Watcher. Network Watcher offers a range of diagnostic tools for Azure networking.



netw

3. In Network Watcher, select Flow Logs. Then, click the Create button to configure the flow logs.



Subscription equals **all** · Resource group equals **all** · Location equals **all**

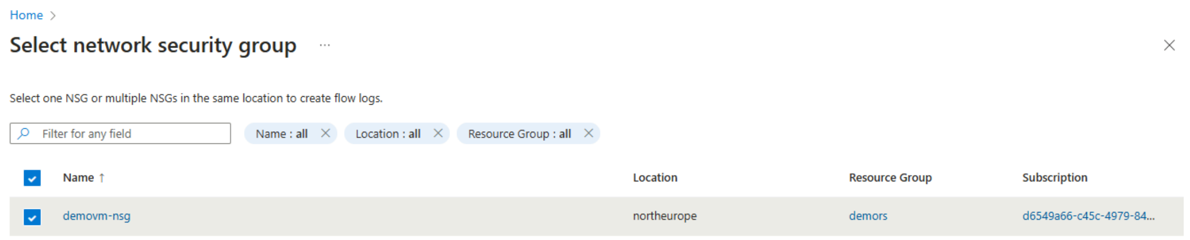
Showing 0 to 0 of 0 records.

Name	Provisioning state	Resource group	Location	Subscription	Status	Flow log type

No flow logs to display

Try changing or clearing your filters.

4. Choose the **NSG** attached to the virtual machine's network interface.Confirm the NSG selection and then Specify the **Azure Storage Account** where flow logs will be saved. Optionally, set a retention period for the logs.



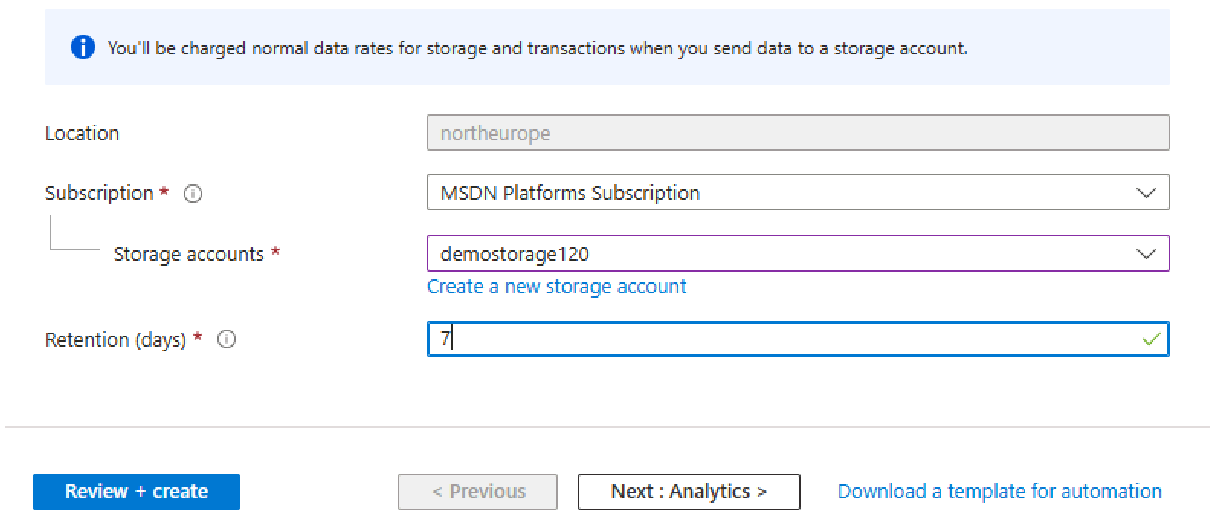
Home >

Select network security group ···

Select one NSG or multiple NSGs in the same location to create flow logs.

Filter for any field | Name : all | Location : all | Resource Group : all

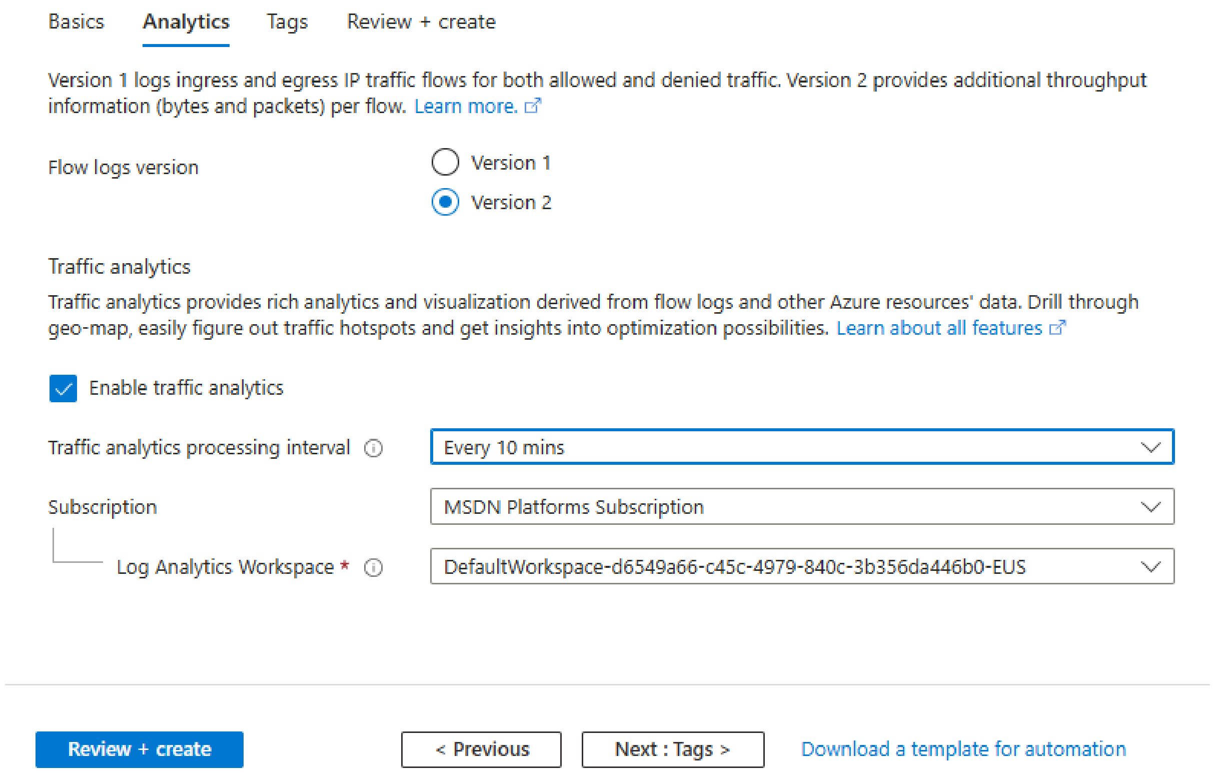
☑	Name ↑	Location	Resource Group	Subscription
☑	demovm-nsg	northeurope	demors	d6549a66-c45c-4979-84...



You'll be charged normal data rates for storage and transactions when you send data to a storage account.

Location	northeurope
Subscription *	MSDN Platforms Subscription
Storage accounts *	demostorage120
	Create a new storage account
Retention (days) *	7

5. Utilize Version 2 to obtain more comprehensive logging information. Activate Traffic Analytics if necessary for in-depth processing and visualization at ten-minute intervals. Examine the configurations and select Create to activate the flow logs.



Version 1 logs ingress and egress IP traffic flows for both allowed and denied traffic. Version 2 provides additional throughput information (bytes and packets) per flow. Learn more.

Flow logs version ○ Version 1 ● Version 2

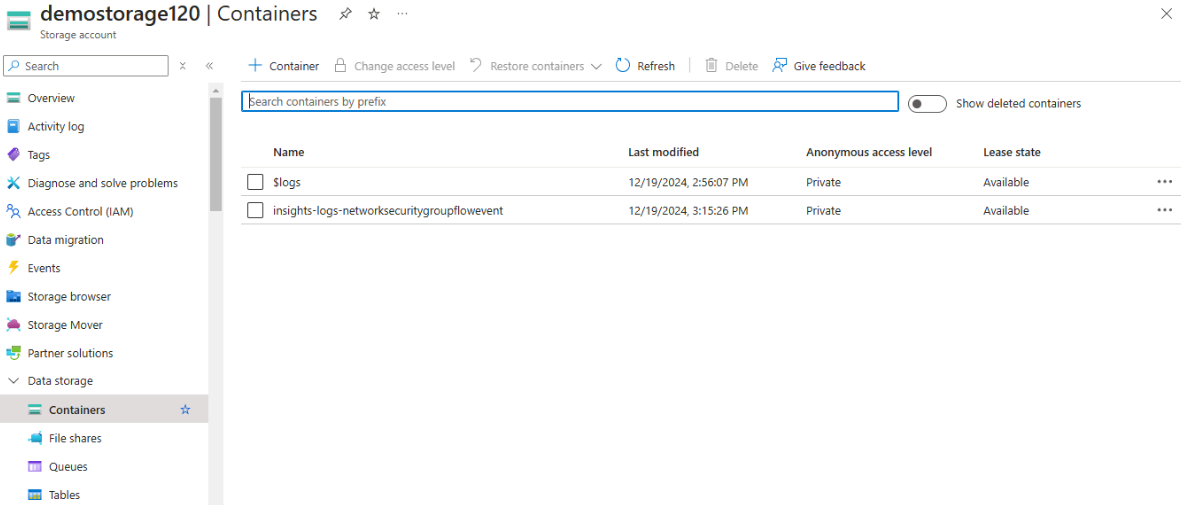
Traffic analytics

Traffic analytics provides rich analytics and visualization derived from flow logs and other Azure resources' data. Drill through geo-map, easily figure out traffic hotspots and get insights into optimization possibilities. Learn about all features

☑ Enable traffic analytics

Traffic analytics processing interval	Every 10 mins
Subscription	MSDN Platforms Subscription
Log Analytics Workspace *	DefaultWorkspace-d6549a66-c45c-4979-840c-3b356da446b0-EUS

6. Now allow a minimum of 30 minutes for the generation and saving of logs. Access the designated Azure Storage Account and proceed to the Containers section. An insights container will be automatically established for the flow logs.

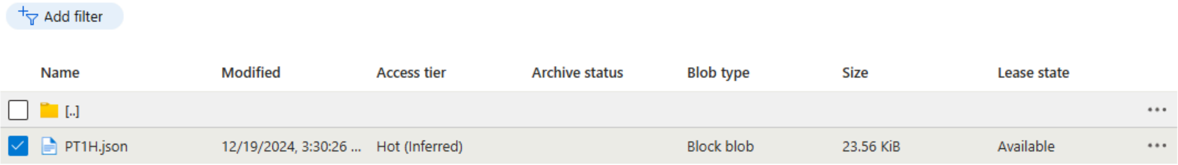


demostorage120 | Containers

Storage account

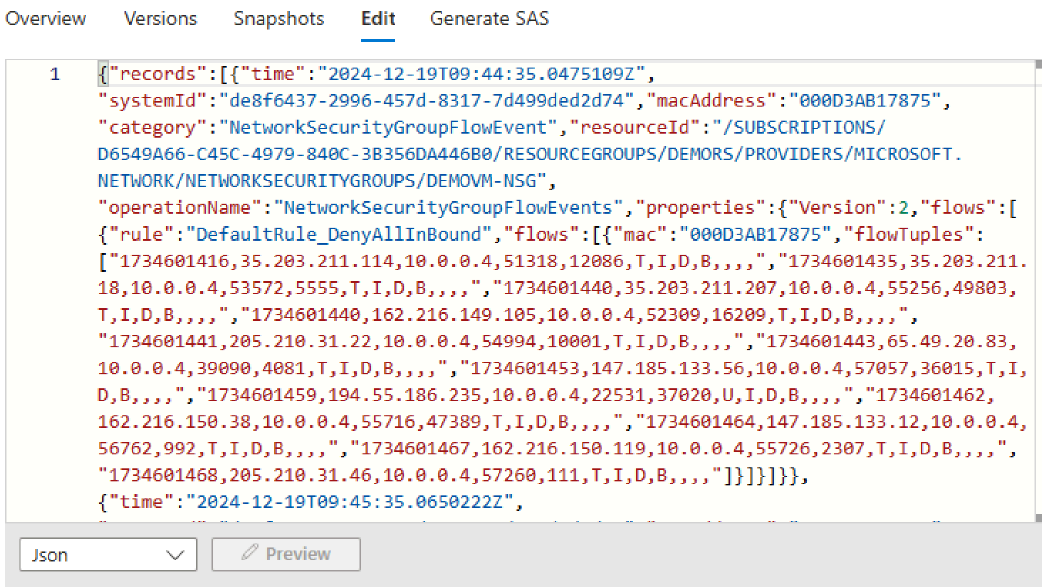
	Name	Last modified	Anonymous access level	Lease state	
□	$logs	12/19/2024, 2:56:07 PM	Private	Available	···
□	insights-logs-networksecuritygroupflowevent	12/19/2024, 3:15:26 PM	Private	Available	···

7. Within the insights container, the folders are structured as follows: Resource ID → Year → Month → Day → Hour. You can find the JSON-based log files within these designated folders.



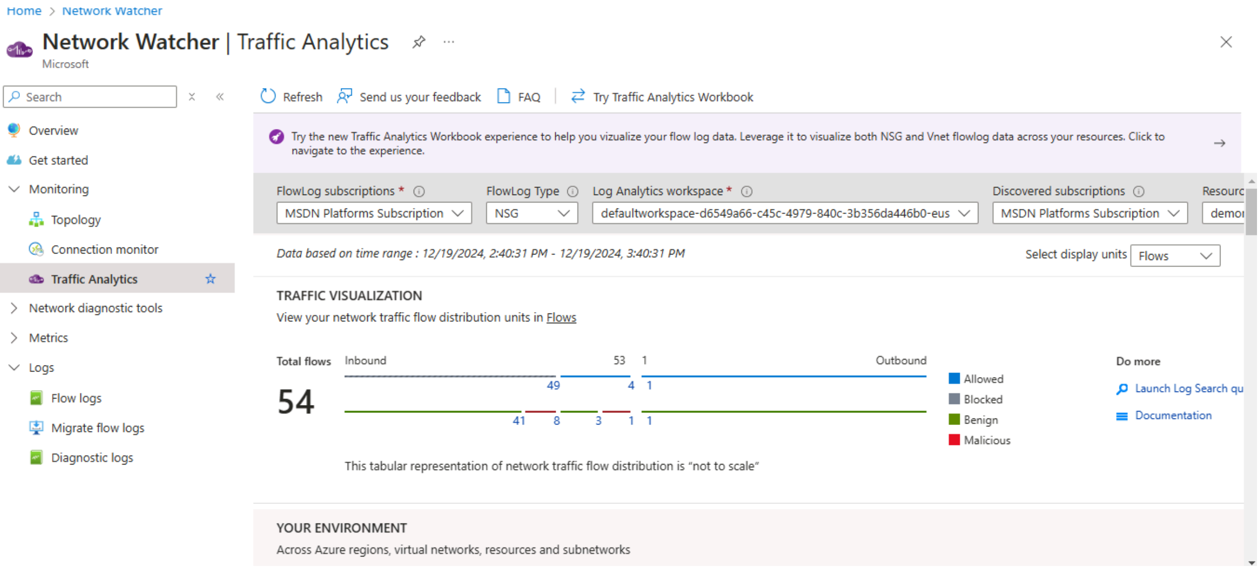
	Name	Modified	Access tier	Archive status	Blob type	Size	Lease state	
□	[..]							···
☑	PT1H.json	12/19/2024, 3:30:26 ...	Hot (Inferred)		Block blob	23.56 KiB	Available	···

8. Access a JSON file to examine flow log entries. Each entry contains information such as **Timestamp:** The moment the request was made.**Source IP Address:** The IP address that initiated the request.**Destination IP Address:** The intended target IP. Action: Whether the traffic was Allowed or Denied.



```
{"records":[{"time":"2024-12-19T09:44:35.0475109Z",
"systemId":"de8f6437-2996-457d-8317-7d499ded2d74","macAddress":"000D3AB17875",
"category":"NetworkSecurityGroupFlowEvent","resourceId":"/SUBSCRIPTIONS/
D6549A66-C45C-4979-840C-3B356DA446B0/RESOURCEGROUPS/DEMORS/PROVIDERS/MICROSOFT.
NETWORK/NETWORKSECURITYGROUPS/DEMOVM-NSG",
"operationName":"NetworkSecurityGroupFlowEvents","properties":{"Version":2,"flows":[
{"rule":"DefaultRule_DenyAllInBound","flows":[{"mac":"000D3AB17875","flowTuples":
["1734601416,35.203.211.114,10.0.0.4,51318,12086,T,I,D,B,,,,","1734601435,35.203.211.
18,10.0.0.4,53572,5555,T,I,D,B,,,,","1734601440,35.203.211.207,10.0.0.4,55256,49803,
T,I,D,B,,,,","1734601440,162.216.149.105,10.0.0.4,52309,16209,T,I,D,B,,,,",
"1734601441,205.210.31.22,10.0.0.4,54994,10001,T,I,D,B,,,,","1734601443,65.49.20.83,
10.0.0.4,39090,4081,T,I,D,B,,,,","1734601453,147.185.133.56,10.0.0.4,57057,36015,T,I,
D,B,,,,","1734601459,194.55.186.235,10.0.0.4,22531,37020,U,I,D,B,,,,","1734601462,
162.216.150.38,10.0.0.4,55716,47389,T,I,D,B,,,,","1734601464,147.185.133.12,10.0.0.4,
56762,992,T,I,D,B,,,,","1734601467,162.216.150.119,10.0.0.4,55726,2307,T,I,D,B,,,,",
"1734601468,205.210.31.46,10.0.0.4,57260,111,T,I,D,B,,,,"]}]}]}},
{"time":"2024-12-19T09:45:35.0650222Z",
```

9. Use Azure documentation to interpret JSON fields in flow log records.
10. Go to **Network Watcher → Traffic Analytics**. Allow time (up to 1 hour) for data to aggregate in **Log Analytics Workspace**.



Home > Network Watcher

Network Watcher | Traffic Analytics

Microsoft

Try the new Traffic Analytics Workbook experience to help you vizualize your flow log data. Leverage it to visualize both NSG and Vnet flowlog data across your resources. Click to navigate to the experience.

FlowLog subscriptions *: MSDN Platforms Subscription

FlowLog Type: NSG

Log Analytics workspace *: defaultworkspace-d6549a66-c45c-4979-840c-3b356da446b0-eus

Discovered subscriptions: MSDN Platforms Subscription

Resourc: demo

Data based on time range : 12/19/2024, 2:40:31 PM - 12/19/2024, 3:40:31 PM

Select display units: Flows

TRAFFIC VISUALIZATION

View your network traffic flow distribution units in Flows

This tabular representation of network traffic flow distribution is "not to scale"

YOUR ENVIRONMENT

Across Azure regions, virtual networks, resources and subnetworks

11. Traffic Analytics offers the following insights: **Traffic distribution:** A comprehensive overview of network traffic. **Malicious traffic detection**: Identification of potential threats. In-depth visualizations of traffic patterns.