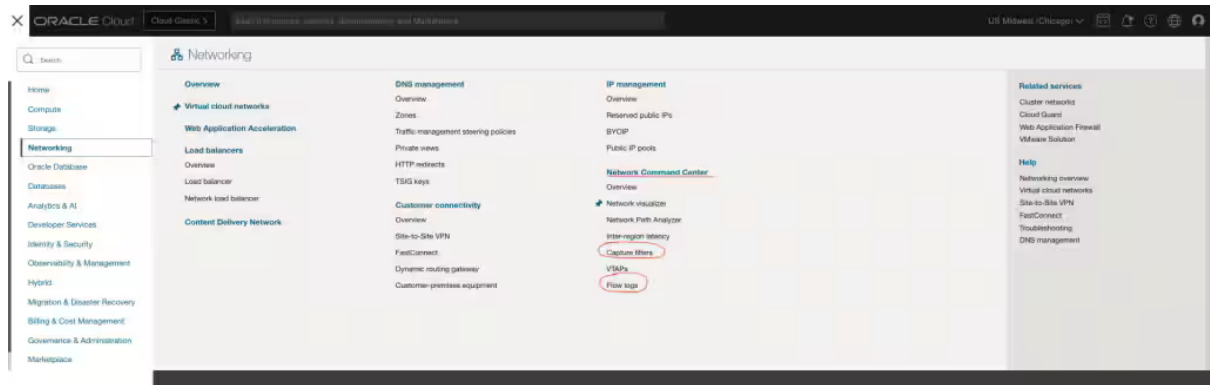


# OCI Flow Logs Unveils Enhancements To Streamline Your Network Monitoring Experience

October 11, 2023

We're pleased to announce the general availability of exciting new features for Oracle Cloud Infrastructure (OCI) flow logs in all commercial regions. These features offer simplified user experience, granular filtering option and targeted enablement. You can find these enhancements in the Oracle Cloud Console under Networking in the Network Command Center.



Flow logs play a crucial role in activities such as monitoring, troubleshooting, security analysis and developing a deeper understanding of your network’s behavior. In busy networks, a mountain of real-time network traffic is at hand. Capturing purposeful real-time network flow data can be unruly, like trying to find a needle in a haystack without a magnet. Flow logs now offer a new simplified user experience that include configuration controls, such as capture filters and targeted enablement points, to help ensure that valuable information doesn’t get lost in the overwhelming clutter.

Previously, we announced [“Announcing VCN flow logs general availability for Oracle Cloud Infrastructure,”](#) written by [Paul Cainkar](#) and [“Working with Flow Logs,”](#) written by [Ajay Chhabria](#). This post explores the latest enhancements for flow logs.

## Common use cases and benefits

Network flow logs with capture filters and enablement points are essential tools for monitoring and managing network traffic. They provide detailed information about the flow of data packets within a network, which can be valuable for various use cases. Network flow logs with capture filters and enablement points have the following common use cases:

- **Network performance:** Capturing and analyzing network flows allows network administrators to identify bandwidth hogs, optimize routing, understand traffic distribution across geographies, perform capacity planning and troubleshoot performance issues.
- **Troubleshooting and debugging:** When network issues occur, flow logs with capture filters can provide detailed information about the affected connections, helping diagnose and resolve problems more quickly. You can use enablement points to trigger packet captures for specific flows, allowing for in-depth analysis of network issues.

- **Capacity planning:** Analyzing network flow logs helps organizations forecast future bandwidth requirements and plan for network capacity upgrades as needed. Flow logs can aid in determining which applications or services are consuming the most resources, allowing for efficient resource allocation.
- **Network security analytics:** You can use flow logs to establish a baseline of normal network traffic and then detect deviations or anomalies that can indicate security breaches or unusual activities. Analyzing flow logs with capture filters helps identify suspicious or malicious network activities by tracking connections to known malicious IP addresses or patterns of behavior.
- **Regulatory compliance:** Organizations can retain and archive network flow logs for compliance purposes, helping them demonstrate adherence to regulatory requirements by providing a record of the network activity. Use network flow logs to track and audit user access to sensitive resources, helping ensure compliance with access control policies.

Using network flow logs with capture filters and enablement points, organizations can gain valuable insights into their network's operation, security, and performance.

## Getting started

Each flow log configuration consists of the two new components: Capture filters and targeted enablement points.

## Capture filter

Previously, we announced capture filters as part of our virtual test access point (VTAP) service. You can learn more about the VTAP feature and use cases by reading the post, "[Announcing VTAP for Oracle Cloud Infrastructure](#)," written by [Misha Kasvin](#). Today, we're announcing the use of capture filters with flow logs. A capture filter is a powerful feature that controls granularity and contains a set of rules governing how traffic is captured by a flow log. A capture filter is associated with a flow log configuration and defines what type of traffic to capture.

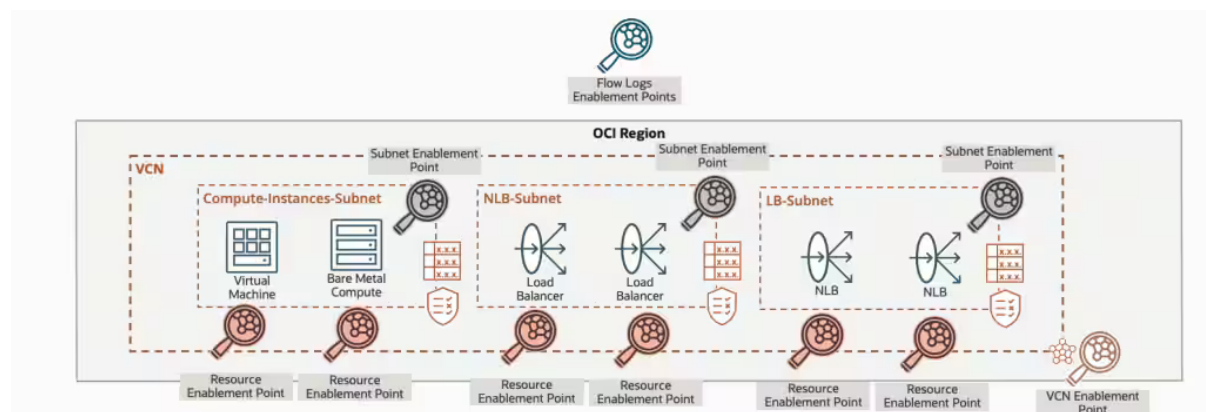
You can create multiple rules inside a capture filter with include or exclude actions, such as direction (ingress and egress), source and destination CIDRs, protocol (TCP, UDP, and ICMP), source, and destination port. Capture filters for flow logs also include a sampling rate to control of the volume of traffic captured. Rules inside a capture filter are analyzed top to bottom, like with an

access list, to determine what traffic is captured. A flow log must have a capture filter associated with it, and each capture filter must have at least one rule.

## Targeted enablement points

Capturing flow data from all resources within a subnet or virtual cloud network (VCN) might not be required or useful. For example, for a subnet that contains production and development servers, you might only need to collect flow logs from the production servers. You can now select specific capture points from where flow logs are collected. The following enablement points are supported:

- One or more existing VCNs: When specific VCNs are selected as enablement points, flow logs are collected from all subnets and resource virtual network interfaces (VNICs) in the current and future subnets. Use this feature when you want to capture flows from the broadest source of information for your network, including flows for all network subnets and all network resources in those subnets. See the VCN enablement point in the following figure.
- One or more existing subnets: When specific subnets are selected for a VCN, flow logs are collected from all VNICs that exist within current and future subnets including resource VNICs, such as Compute instances, load balancers, and network load balancers (NLBs). Use this point when you want to capture only flows from a particular subnet. See the subnet enablement point in the following figure.
- One or more existing resources: When specific resources are selected for a VCN and within a subnet, flow logs are collected from only those resource VNICs, such as Compute instances, load balancers, and NLBs. Use this feature when you only want to capture flows from a particular subnet. See resource enablement point in the following figure.

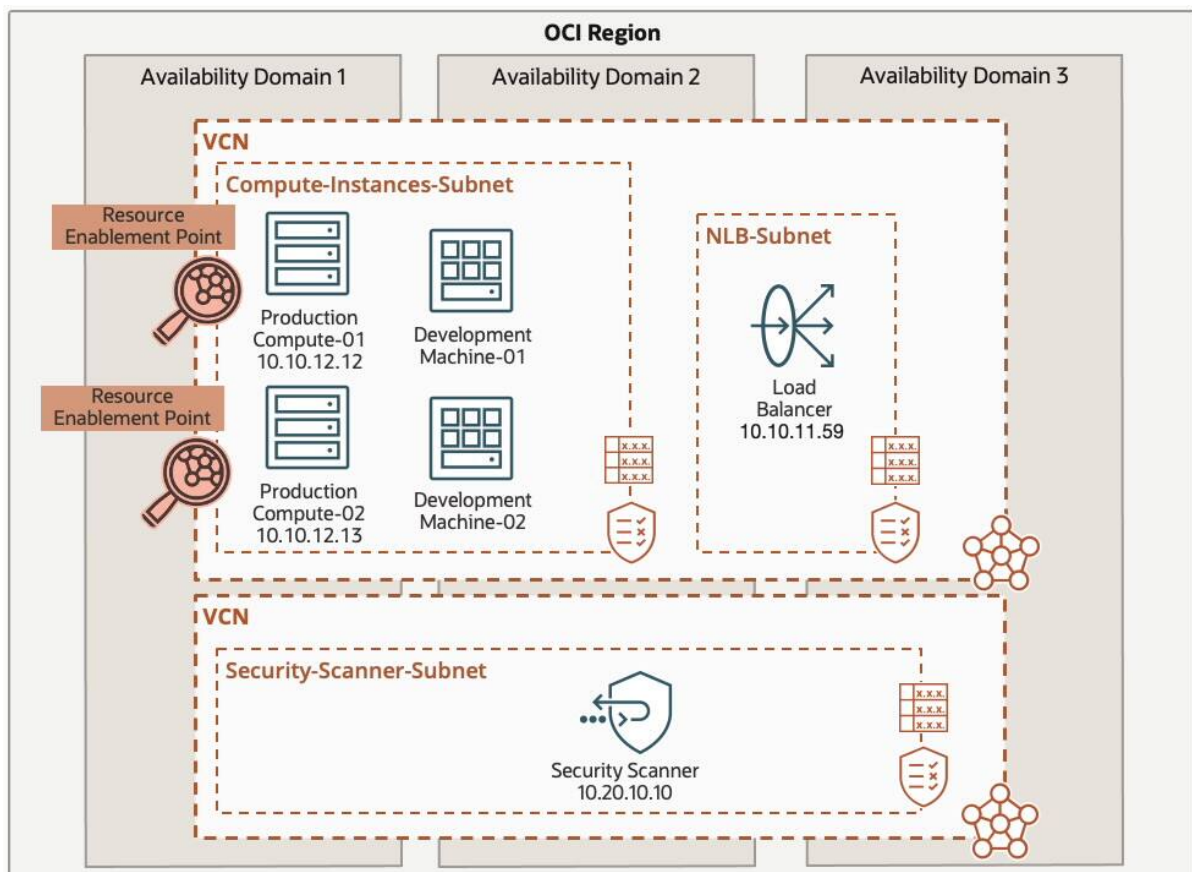


Existing flow logs within your VCN are automatically migrated under flow log configurations to align with these new enhancements. They're enabled at the subnet level and use a hidden default capture filter set to capture all network flows to ensure backwards compatibility with previous behavior. The following example shows existing flow logs that have been migrated.

## Sample use case and setup

Now that we've covered the basics, let's discuss a sample use case. Using the topology, you have a Compute subnet that contains both production and development Compute instances. You also have a NLB subnet that contains the NLB frontending the production backend Compute instances. Lastly, a security scanner subnet hosts a security scanner.

You want to capture only 25% of the flows coming from the NLB to the production backend compute instances on only TCP port 8080 and exclude everything else, like the flows from the security scanner.

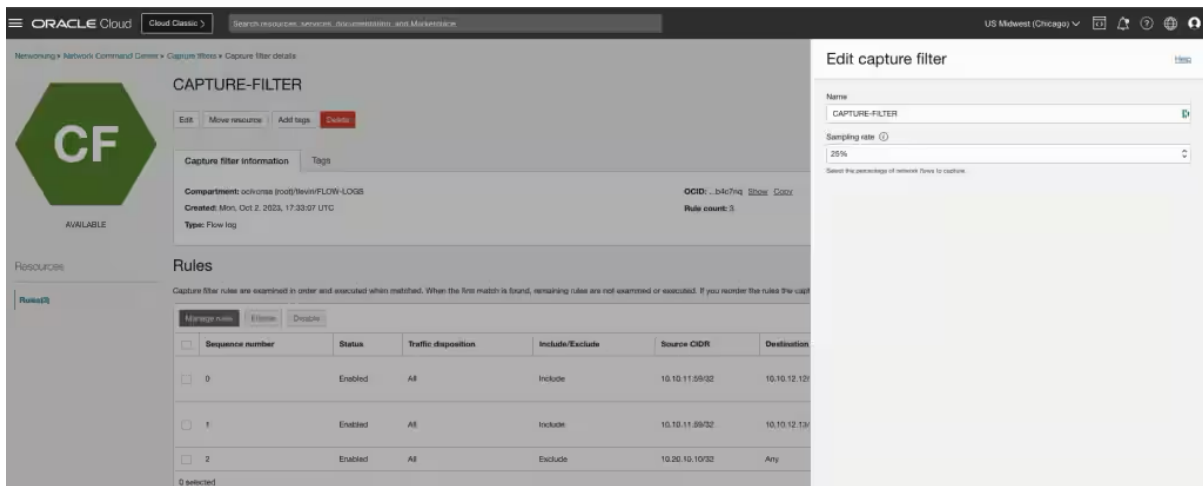


# Create capture filter

To start the configuration workflow, you can access for flow logs in the navigation menu in the Console, under Networking and Network Command Center, select **Capture filters**.

Create a flow log capture filter type that captures 25% of the traffic flows with the following capture rules:

- Include Source CIDR 10.10.11.59/32 (NLB) → Destination CIDR 10.10.12.12/32 (Production Compute-01)
- Include Source CIDR 10.10.11.59/32 (NLB) → Destination CIDR 10.10.12.13/32 (Production Compute-02)
- Exclude Source CIDR 10.20.10/32 (Security Scanner) → Destination CIDR Any



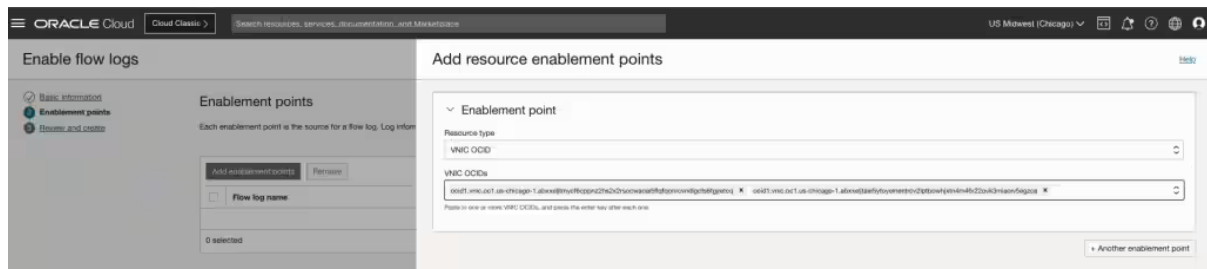
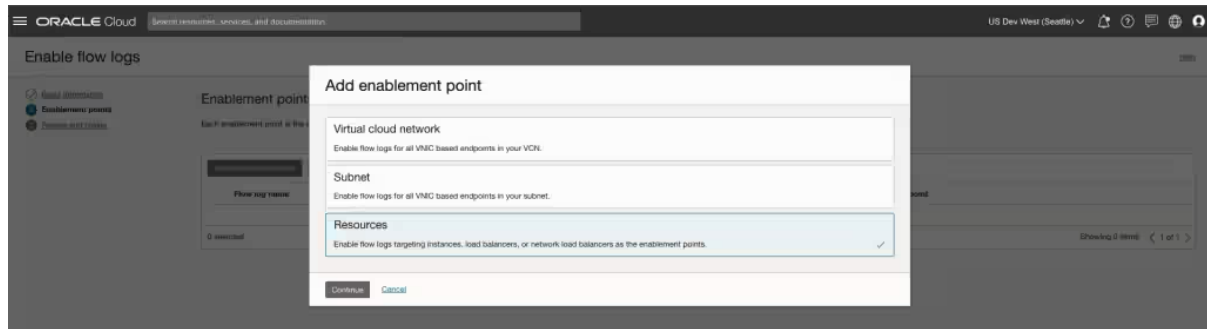
The screenshot shows the Oracle Cloud console interface for editing a capture filter. The main area displays the 'CAPTURE-FILTER' resource details, including its name, compartment, creation time, and type. The 'Rules' section is expanded, showing a table of three rules. The 'Edit capture filter' sidebar on the right shows the filter name and a sampling rate of 25%.

| Sequence number | Status  | Traffic disposition | Include/Exclude | Source CIDR    | Destination |
|-----------------|---------|---------------------|-----------------|----------------|-------------|
| 0               | Enabled | All                 | Include         | 10.10.11.59/32 | 10.10.12.12 |
| 1               | Enabled | All                 | Include         | 10.10.11.59/32 | 10.10.12.13 |
| 2               | Enabled | All                 | Exclude         | 10.20.10/32    | Any         |

# Enable flow logs for enablement points

To start the configuration workflow, you can access for flow logs in the navigation menu in the Console, under Networking and Network Command Center, select **Flow logs**.

Enable flow logs and use the Resource enablement point to enable flow logs using either the VNIC OCIDs or Instance VNICs.



You can now see the flow log configurations under in the Network Command Center. After the flow logs have been configured and started, you can access, search, filter and visualize your logs from the Oracle Cloud Logging Search experience. You can also use a third party streaming tool to receive captured traffic flows as described in the "[Announcing VCN flow logs general availability for Oracle Cloud Infrastructure](#)" and "[Working with Flow Logs](#)" blogs.

## Conclusion

We're pleased to bring you this new dynamic and flexible solution for your capturing needs. We look forward to hearing about how this feature improves your user experience and network monitoring, troubleshooting, and security analysis goals.

We encourage you to explore these new features and all the enterprise-grade capabilities that Oracle Cloud Infrastructure offers. You can share any product feedback that you have through email to the [Virtual Networking group](#) or submit a note in the comments.

To learn more, see the following resources:

- [Exporting VCN Flow Logs into OCI Logging Analytics](#)
- [How to Ingest OCI VCN Flow Logs into OCI Logging Analytics](#)
- [Announcing stream and log processing in Service Connector Hub](#)

- Oracle Cloud Infrastructure Service Connector Hub now generally available

## About Cloudsway

Cloudsway is a subsidiary of Wangsu Science and Technology (stock code: 300017), established in March 2023. Wangsu Science and Technology is a global leading provider of information infrastructure platform services, with business spread across more than 70 countries and regions worldwide.

Cloudsway is one of the three innovation engines in Wangsu's "2+3" strategy, providing enterprises with integrated products and solutions, such as cloud strategy consulting, modernized application construction, generative AI, and enterprise-grade cloud hosting services. solutions based on AWS.

Cloudsway is committed to become a leading provider of hybrid cloud solutions, offering secure, efficient, and convenient cloud services to enterprises, helping them with digital and intelligent transformation, and boosting their operational efficiency.