

# ExtraHop QuickStart Guide

## Basic Navigation

### Where are my systems?

- Devices » Find
- Device Groups » Activity Groups
- Device Groups » User Groups

To configure user groups:

1. Go to **Devices » Find** (search by substring).
2. Click **All** or check a few devices.
3. Click **Add To Group**.

- Summary

To configure:

1. Configuration » New Dashboard
2. Find a device, **Add to Summary**

### What is the network utilization?

**Network » L2**

### Who are the top talkers?

**Network » L3**

### What is consuming bandwidth?

**Network » App**

### Which are the busiest servers?

*Example: busiest DB servers*

1. Go to **Device Groups » Activity Groups » Database Servers** or **DB Overview** widget.
2. Click **Requests** to sort table by requests.

### Which are the slowest servers?

*Example: slowest DB servers*

1. Go to **Device Groups » Activity Groups » Database Servers** or **DB Overview** widget.
2. Expand the DB tree control on the left and click **Processing Time**. The ten slowest servers are shown in the histogram.

### Which servers are generating errors?

*Example: DB servers with errors*

1. Go to **Device Groups » Activity Groups » Database Servers** or **DB Overview** widget.
2. Click **Errors** in the table to sort by errors.
3. Click through to the database device that generated the most errors.
4. Select the **DB** tab for database details.
5. Click the red **Errors** button for detailed error messages.

## Configuring Alerts

Go to **Settings » Alerts** to create alerts for metrics that affect business-critical transactions (refer to the *ExtraHop Alerts Guide* for details).

## Basic Troubleshooting

### Slowness: Is it the server or the network?

Navigate to the server, pick a function for which the server is responsible (for example, **HTTP**), and select the metric type **Server**.

1. Check the Transaction Metrics chart:
  - If Req/Rsp Xfer is large, the network is slow.
  - If Processing Time is large, the server is slow.
2. If there are additional tiers to which this server makes requests, select that protocol (for example, **DB**) and then select the metric type **Client**.

Check the Transaction Metrics chart:

- If times are large, the next tier is slow.
  - Otherwise, the current server is slow.
3. Check what is taking a long time on server:
    - *HTTP*—Select “By URI” in the **HTTP Details** dropdown. Click **Responses** for per-URI breakdown.
    - *DB*—Click the **Methods** button to see per table and stored procedure breakdown.
    - *CIFS, NFS, FTP*—Click the **Files** button to see which files have been transferred.
    - *DNS*—Click the **Host Queries** button to see which entries have been queried.

### Congestion: Where is it?

1. **Device Groups » Activity Groups » TCP**

RTOs are a good indicator of congestion (click **Help** for other examples).

2. Click In: **RTOs** and Out: **RTOs** to see which devices have the most RTOs.
3. Click the device that has the most RTOs and then click **TCP** to go to its TCP properties.
4. To see the devices from which RTOs are coming, click **RTOs** in the device view.

## Aborted connections: Which device is aborting?

1. Go to **Device Groups** » **Activity Groups** » **TCP**.
2. Click **Out: Aborts** to see which devices aborted the most connections.
3. Click the device that has the most aborts and then click **TCP** to go to its TCP properties
4. To see the devices to which aborts were sent, click **Aborts** in the device view.

## More Information

Click **Help** in the top-right corner of any screen to open context-sensitive Help, which explains every metric in detail. Contact [support@extrahop.com](mailto:support@extrahop.com) for questions and additional user guides.