Product Version: Since nChronos 3.0

Intended Audience:

- All nChronos users (including *Evaluation* users)

In last tutorial we've learned:

1. How to connect to a nChronos server from console
2. How to troubleshoot connection error issues

Before heading into this chapter, please make sure you've fully got the answers to these questions. If you have doubts about them, you are recommended to go back to take a look at last chapter first, or you can turn to us for help on your specific case.

In this chapter we'll take a look at the user interface of nChronos Console. nChronos Console is the component that we use to view network analysis stats, perform drill-down analysis and also manage server settings, etc. So we use nChronos Console more often that the server program. When we run the console program first we come to the *Start Page*, where we can find the latest official news, product documents, learning resources and the contact info. If we add a server connection (more details on last chapter) on the **Server Explorer** (left-side panel), we can connect to the server, and it opens the stats view. The view contains a **trend chart** and several stats views.

Packet File Explorer

In last chapter we've learnt what Server Explorer is. If you look down under this panel, you can find there is something called **Packet File Explorer**. This is another important function that not only monitoring real-time traffic traveling through your network by nChronos server, nChronos console has the ability to analyze the packet files (also known as trace files). nChronos console supports to open the packet files generated by Colasoft portable network analyzer – Colasoft
Capsa
(also the packets downloaded from nChronos Server), and
.cap
and
.pcap
files by Wireshark. This is useful when we have a large sized packet file, and we just need to concentrate on a part of the packet file. We use nChronos console to open the file and lock down to the specific time period and analyze into the packets of that period.

So it means we can analyze traffic either from real-time capture, or also from packet files. And we use same experience to analyze them with the following given views.

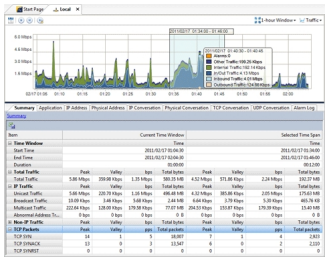
The Trend Chart (Time Window)

The trend chart and the time window are the same thing. With the trend charts, we are able to have a graphical view of traffic trends. It helps us identify when the traffic drops and when climbs more visually than just numbers, and then we can focus on the abnormal time period to see what happened during that period closely. So it's often the starting point where we start out retrospective and drill-down analysis. By default, the time window shows the traffic trend of past four minutes. When we change or move the time window, the chart refreshes automatically. We can zoom in to time unit of second and zoom out to hour, which means if we have a 4-minute time window we can view traffic stats of every second, while 10-day window shows stats of each hour.

If we are interested in looking into a specific time period, we can *click and drag* to select a time span on the trend chart to view traffic statistics of that period. By selecting a time span on the trend chart, the views down below displays only the statistics of that time period, it helps us focus on only that small slice of time. For example, we are reported that users cannot access the webserver at about 7:00 AM to 7:15 AM, and we need to figure out the causes of this downtime. Now we can connect to nChronos server, and rewind back to the time window of that period, select time period between 7:00 – 7:15. And the views will refresh to show the traffic statistics between those 15 minutes. Next we can analyze by using the drill-down feature to focus on the webserver address, and check if its data link layer, Internet layer, and its TCP transports are stable.

Statistic Views

There are several views below the trend chart which display types of statistics in different tabs. They work together with trend charts and time span selection to reduce statistic data volumes and let us focus on analyzing and drill-down to look into network issues. The views are described below:



1. **Summary** view: overall summary statistics of alarms, total traffic, inbound traffic, outbound traffic, IP and non-IP traffic and TCP packets statistics. If you select a time span on the trend chart, the summary statistics of this time span are displayed on the right side.

2. **Application** view: traffic statistics of network applications, such as TCP, HTTP, POP3, etc.
3. **IP Address** view: traffic statistics based on every IP address, including bytes, packets, pps, etc.
4. **Physical Address** view: traffic statistics based on every MAC address, including bytes, packets, pps, etc.
5. **IP Conversation** view: traffic statistics on IP address pairs. You can know which nodes are communicating and their connection statistics.
6. **Physical Conversation** view: traffic statistics on MAC address pairs.
7. **TCP Conversation** view: statistics, on the transport layer, of the IP addresses and ports, including packets sent and received, conversation duration, Bps etc.

8. **UDP Conversation** view: statistics, another important transport layer protocol, of the IP addresses and ports, including packets sent and received, conversation duration, Bps etc.

9. **Alarm Log** view: the log records of the alarm trigger and release records.

The views above mentioned, except the Summary view, will have records displayed only when you select a time span on the trend chart. And when you change the selection of the time span, the statistics on the views will refresh automatically. And you can select records in the views

and right-click to select drill-down analysis, by this way, you are able to focus on specific network objects and find the source of what you want.

So far, we can see that nChronos console user interface is clear and simple to understand and we are going to talk about how to use the console program in next chapter.