

NetkaView Logger

Netka System

NetkaView Logger | NLG-SW | บริษัท เน็ตก้า ซิสเต็ม จำกัด

อุปกรณ์เก็บรักษาข้อมูล จราจรทางคอมพิวเตอร์

ได้รับการรับรองตามมาตรฐาน มคอ. 4003.1-2560

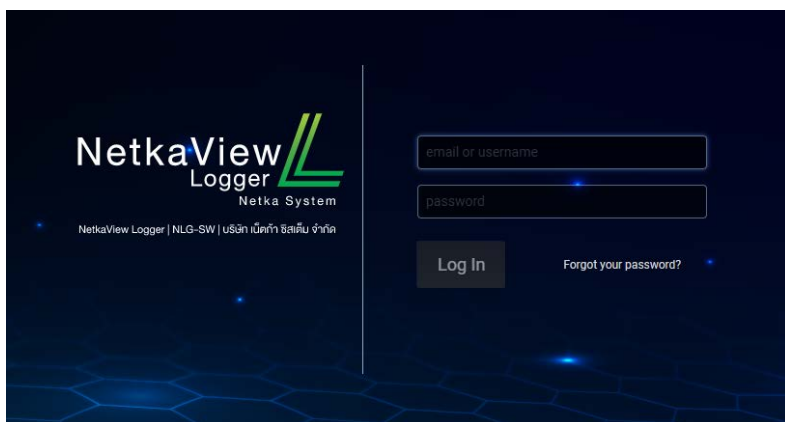
จุดเด่นของผลิตภัณฑ์

- ออกแบบมาเพื่อเก็บบันทึกการทำงานระบบแบบรวมศูนย์
- รองรับการเก็บข้อมูลบันทึกการทำงานด้วยมาตรฐาน Syslog Protocol RFC5424
- สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS, Command Line Interface และ SSH
- มีหน้าแสดงจอภาพรวมเพื่อประโยชน์ในการเฝ้าดูบันทึกจากแหล่งต่างๆ
- ซอฟต์แวร์รองรับการติดตั้งบนเครื่องแม่ข่ายจริงและเครื่องแม่ข่ายเสมือนจริง (virtual machine)
- สามารถแจ้งเตือนผ่านอีเมล
- สามารถสำรองข้อมูล (Data Backup) เพื่อไปเก็บที่ External Storage พร้อมตรวจสอบความถูกต้องของไฟล์ด้วย Hashing เช่น MD5, SHA-1, SHA-256
- สามารถกำหนดเวลามาตรฐานด้วย NTP
- สามารถควบคุมระยะเวลาการเก็บข้อมูล (Data retention) และการส่งออกข้อมูล (Export) แบบอัตโนมัติ

NetkaView Logger หรือ NLG

เป็นอุปกรณ์เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผ่านการทดสอบและได้รับการรับรองตามข้อกำหนดของมาตรฐาน มคอ.4003.1-2560 “ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์” โดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ซึ่งเป็นข้อกำหนดที่ถูกพัฒนาโดยอ้างอิงพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

NetkaView Logger สามารถรับ เก็บบันทึก และรักษาคุณภาพข้อมูลจราจรทางคอมพิวเตอร์ตามหลักการที่ถูกต้องโดยชอบด้วยกฎหมาย เพื่อลดความเสี่ยงต่อการสูญเสียความถูกต้องสมบูรณ์ของข้อมูล (Data Integrity) และเพียงพอสำหรับระบุผู้เกี่ยวข้องได้อย่างน่าเชื่อถือ



คุณสมบัติของผลิตภัณฑ์ NLG

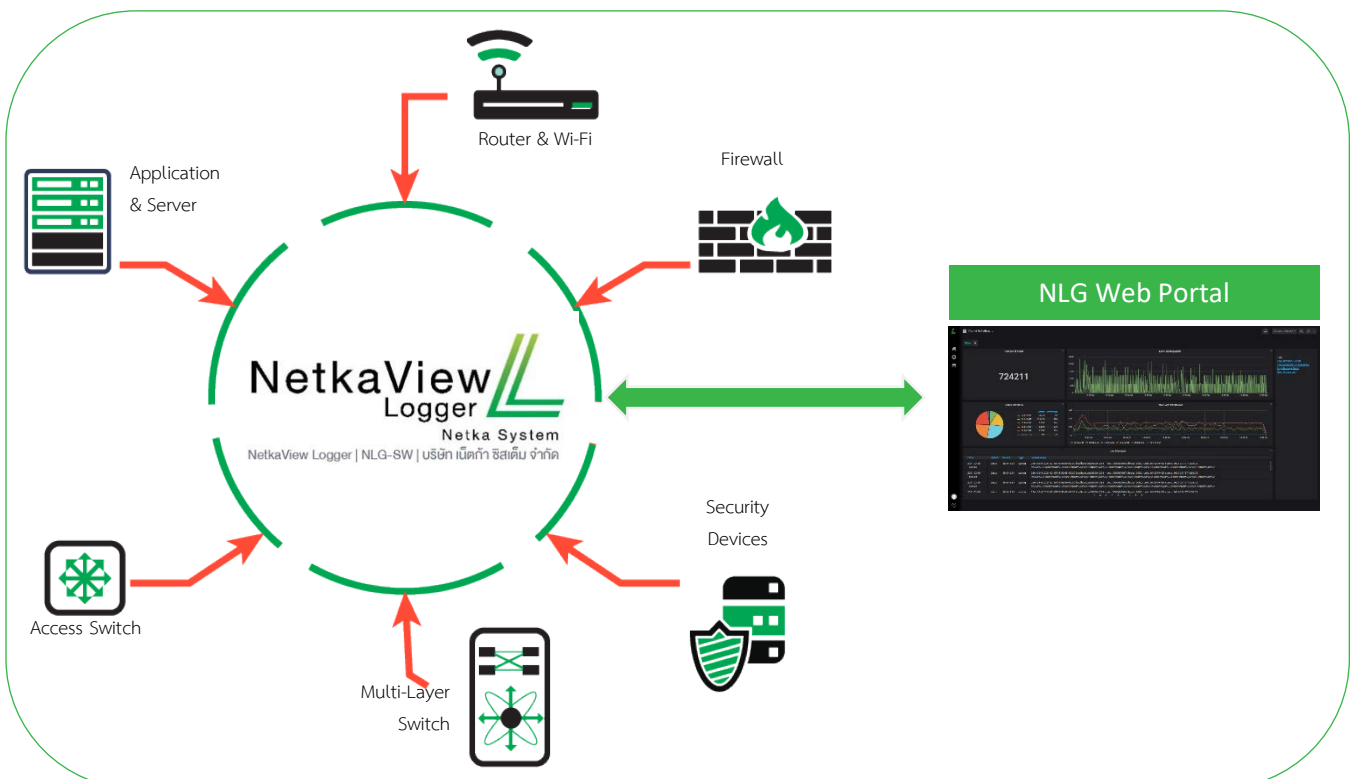
NetkaView Logger (หรือ NLG) เป็นซอฟต์แวร์หรือ Appliance ที่ได้รับการออกแบบมาให้มีคุณสมบัติความสามารถในการรับข้อมูลเหตุการณ์ที่เกิดขึ้นทางคอมพิวเตอร์ในรูปแบบบันทึกเหตุการณ์หรือ Log จากระบบต่างๆ เช่น Switch, Router, Firewall, VPN, Network devices, Server, OS, Database เป็นต้น เพื่อเก็บรวบรวมข้อมูลดังกล่าวไว้ใช้ในการวิเคราะห์เหตุการณ์ที่ปรากฏ ด้วยมาตรฐาน Syslog ซึ่งมีประโยชน์ในการสืบเสาะหาความเกี่ยวพันของข้อมูลจราจรคอมพิวเตอร์ เช่น ข้อมูลบันทึกการเข้าถึงระบบจากเครื่องลูกข่าย (client) ไปยังเครื่องแม่ข่าย (server) ระบุวันเวลาที่เกิดเหตุการณ์, ระบุแหล่งของเหตุการณ์ เป็นต้น ตามข้อกำหนดของมาตรฐาน มคอ.4003.1-2560 ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์



NLG รองรับการทำงานทั้งบนเครื่องแม่ข่ายจริง (barebone) และบนเครื่องแม่ข่ายแบบเสมือนจริง (virtual machine) บนระบบจำลองเครื่องแม่ข่าย (Hypervisor) เช่น VMware, Microsoft Hyper-V, Redhat KVM, Oracle Virtual Box เป็นต้น ช่วยให้เกิดความยืดหยุ่นต่อผู้ใช้งาน NLG ได้เป็นอย่างดี

การติดตั้ง NLG เพื่อเก็บข้อมูลบันทึกการทำงานของระบบสารสนเทศ

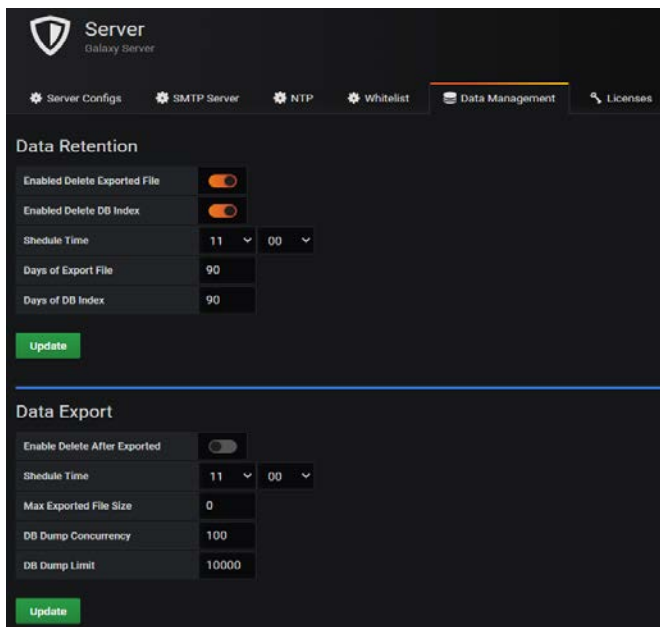
การติดตั้งระบบ NLG ภายในเครือข่ายคอมพิวเตอร์เพื่อเก็บบันทึกการทำงานของระบบ (Log) ให้กับระบบสารสนเทศซึ่งประกอบด้วยอุปกรณ์เครือข่าย เครื่องแม่ข่าย ระบบงาน อุปกรณ์รักษาความปลอดภัย และอุปกรณ์ด้านสารสนเทศอื่นๆ



คุณสมบัติของผลิตภัณฑ์ NLG

Network Time Protocol (NTP)

มีคุณสมบัติในการตั้งค่า Network Time Protocol (NTP) และค่าเวลา Time zone ซึ่งใช้สำหรับการกำหนดเวลามาตรฐาน เพื่อตั้งค่าเวลาของระบบ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ให้ตรงกับเวลามาตรฐานสากล



NTP Informations.

synchronised to NTP server (202.28.93.5) at stratum 2
time correct to within 29 ms
polling server every 256 s

NTP Server.

Server	time.navy.mi.th
Server	time1.nimt.or.th
Server	time2.nimt.or.th
Server	time3.nimt.or.th
Server	clock.nectec.or.th

Update

Time zone.

Time Zone GMT+07:00 Asia/Bangkok

Update

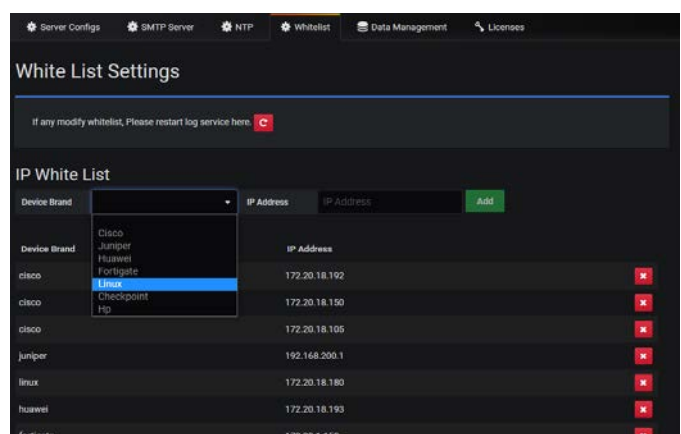
NetkaView Logger | Copyright © 2006 - 2021 Netka System Co.,Ltd. All rights reserved.

Data Management

สามารถบริหารจัดการข้อมูล (Data Management) ซึ่งใช้สำหรับการควบคุมระยะเวลาเก็บข้อมูล (Data retention) และการส่งออกข้อมูล (Export) แบบอัตโนมัติเพื่อเก็บไว้ในพื้นที่จัดเก็บของระบบ

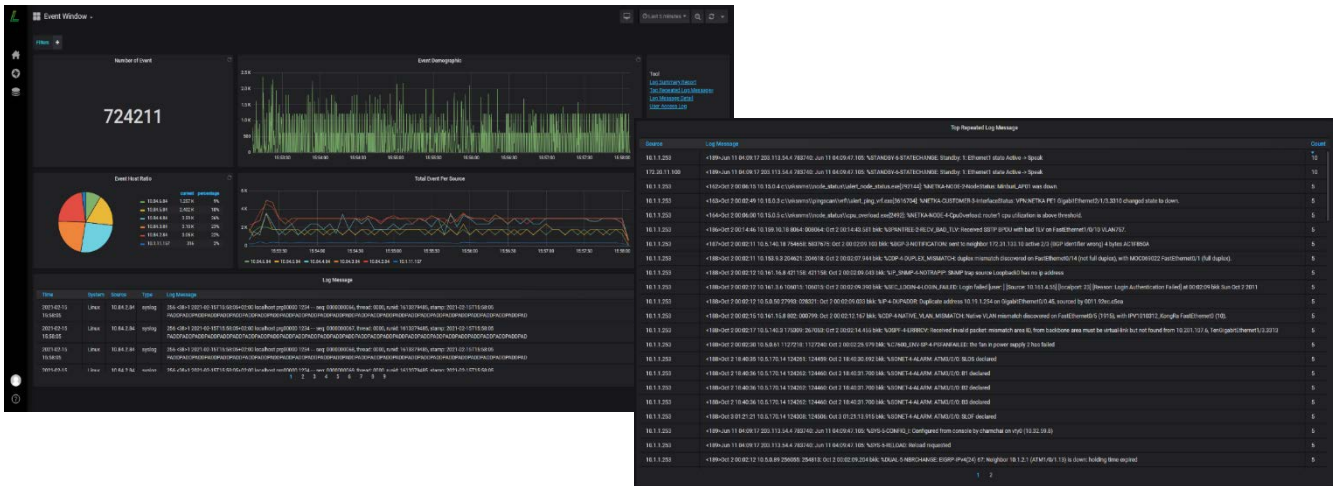
Whitelist / Filtering

หน้าจอเมนู Whitelist ใช้สำหรับการระบุหมายเลข IP address ของอุปกรณ์ หรือเครื่องแม่ข่ายต้นทางที่ NLG จะอนุญาตให้รับข้อมูลจราจรทางคอมพิวเตอร์ (Log or Event) ได้ ช่วยเพิ่ม Security ให้กับระบบ



คุณสมบัติในการวิเคราะห์และแสดงข้อมูล Log จากแหล่งต่างๆ

หน้าจอแสดงผลข้อมูลที่มาจากแหล่งต่างๆ ที่ดูเข้าใจง่ายและสามารถใช้เพื่อค้นหาและวิเคราะห์ข้อมูลได้ง่ายและรวดเร็ว สามารถนำข้อมูลออกจากระบบ (Export) ได้อย่างมีประสิทธิภาพ



คุณสมบัติหลักของเครื่องแม่ข่ายที่แนะนำสำหรับการติดตั้ง NetkaView Logger

Specification	MDES Spec 1	MDES Spec 2	MDES Spec 3
CPU (vCPU)	4 core (8 vCPU)	8 core (16 vCPU)	16 core (32 vCPU)
Memory (GB)	8	16	32
Storage size (TB)	0.5-2	1-7	2-20
Network Interface (port)	1	2	2
จำนวน EPS สูงสุด	1,000	7,000	20,000
ระยะเวลาเก็บข้อมูล	7-90 วัน	7-90 วัน	7-90 วัน

หมายเหตุ:

- ทดสอบภายใต้มาตรฐาน Syslog protocol แบบ UDP ด้วยขนาด packet 256 bytes
- ระยะเวลาการเก็บข้อมูลให้ได้ 90 วัน ขึ้นอยู่กับจำนวน log ที่จัดเก็บ ซึ่งอาจจะต้องมีการเพิ่มขนาด Disk

เลขที่ใบรับรอง 64-0002

ใบรับรองคุณภาพผลิตภัณฑ์

ใบรับรองฉบับนี้ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ออกให้ไว้เพื่อรับรองว่า

ผลิตภัณฑ์

ซอฟต์แวร์เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

Module NLG-MDES-001 เวอร์ชัน 1.X.X

(ที่มีความสามารถในการจัดเก็บข้อมูล เฉพาะตามรายการที่แจ้งแนบท้ายใบรับรองนี้เท่านั้น)

ซึ่งผลิตโดย

บริษัท เน็ตก้า ซิสเต็ม จำกัด

มีสำนักงานอยู่ที่

เลขที่ 1 อาคาร Netka System ซอย รามคำแหง 166 แยก 2 ถนนรามคำแหง แขวงมีนบุรี เขตมีนบุรี
กรุงเทพมหานคร 10510

โทรศัพท์ 0 2978 6805 โทรสาร 0 2978 6909

และมีโรงงานอยู่ที่ ที่เดียวกับสำนักงาน

ซึ่งได้ผ่านการตรวจสอบแล้วพบว่ามีความเป็นไปตามหลักเกณฑ์และเงื่อนไขการรับรองคุณภาพผลิตภัณฑ์ของ
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ และเป็นไปตามข้อกำหนดของมาตรฐานดังนี้

มคอ. 4003.1-2560 ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ เล่ม 1 ข้อกำหนด

ภายใต้ข้อบ่งชี้ผลิตภัณฑ์ที่ระบุข้างต้น บริษัทฯ สามารถนำใบรับรอง และเครื่องหมายรับรองคุณภาพผลิตภัณฑ์ ของ
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ไปใช้ได้ โดยต้อง ปฏิบัติตามหลักเกณฑ์และเงื่อนไขการใช้ใบรับรอง
ทั้งนี้ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ จะดำเนินการตรวจสอบและควบคุมคุณภาพผลิตภัณฑ์ที่ได้รับการ
รับรองนี้ ภายใต้รูปแบบการรับรอง ประเภทที่ 3

วันที่ออกใบรับรอง :

9 กรกฎาคม 2567

วันที่ใบรับรองสิ้นอายุ :

9 กรกฎาคม 2570

(นายชัย วุฒิวิวัฒน์ชัย)

ผู้อำนวยการ

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ให้การรับรองครั้งแรกเมื่อ 9 กรกฎาคม 2564

สถาบันประเมินและรับรองเทคโนโลยีดิจิทัล โทรศัพท์ 0 2564 6900 ต่อ 2083



สวทช.



กมช.-สมอ.-มอก.17065

PRODUCT 001

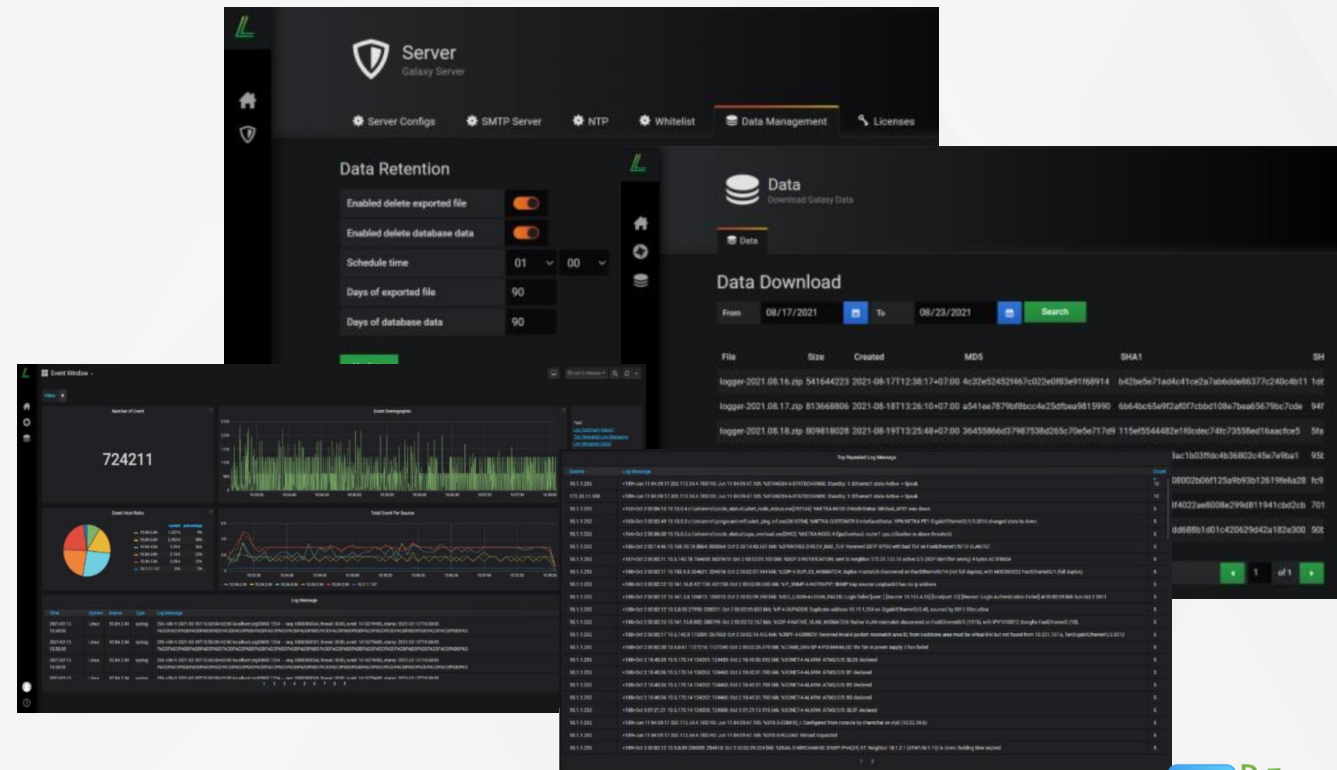
NLG มคอ. 4003.1-2560 (Centralized Log)

NetkaView Logger(NLG) มคอ. 4003.1-2560

เป็นอุปกรณ์เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผ่านการทดสอบและ ได้รับการรับรองตามข้อกำหนดของมาตรฐาน มคอ.4003.1-2560 “ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์” โดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และ คอมพิวเตอร์ แห่งชาติ ซึ่งเป็นข้อกำหนดที่ถูกพัฒนาโดยอ้างอิงพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

Key Features & Product Highlights:

- Real-Time Log monitoring
- Dashboard Datasource, Audit and Raw log
- Export Data
- Comply มคอ.4003.1-2560
- Comply พรบ. คอมพิวเตอร์ พ.ศ. 2560
- ตรวจสอบความถูกต้องของไฟล์ด้วย MD5,SHA,SHA256

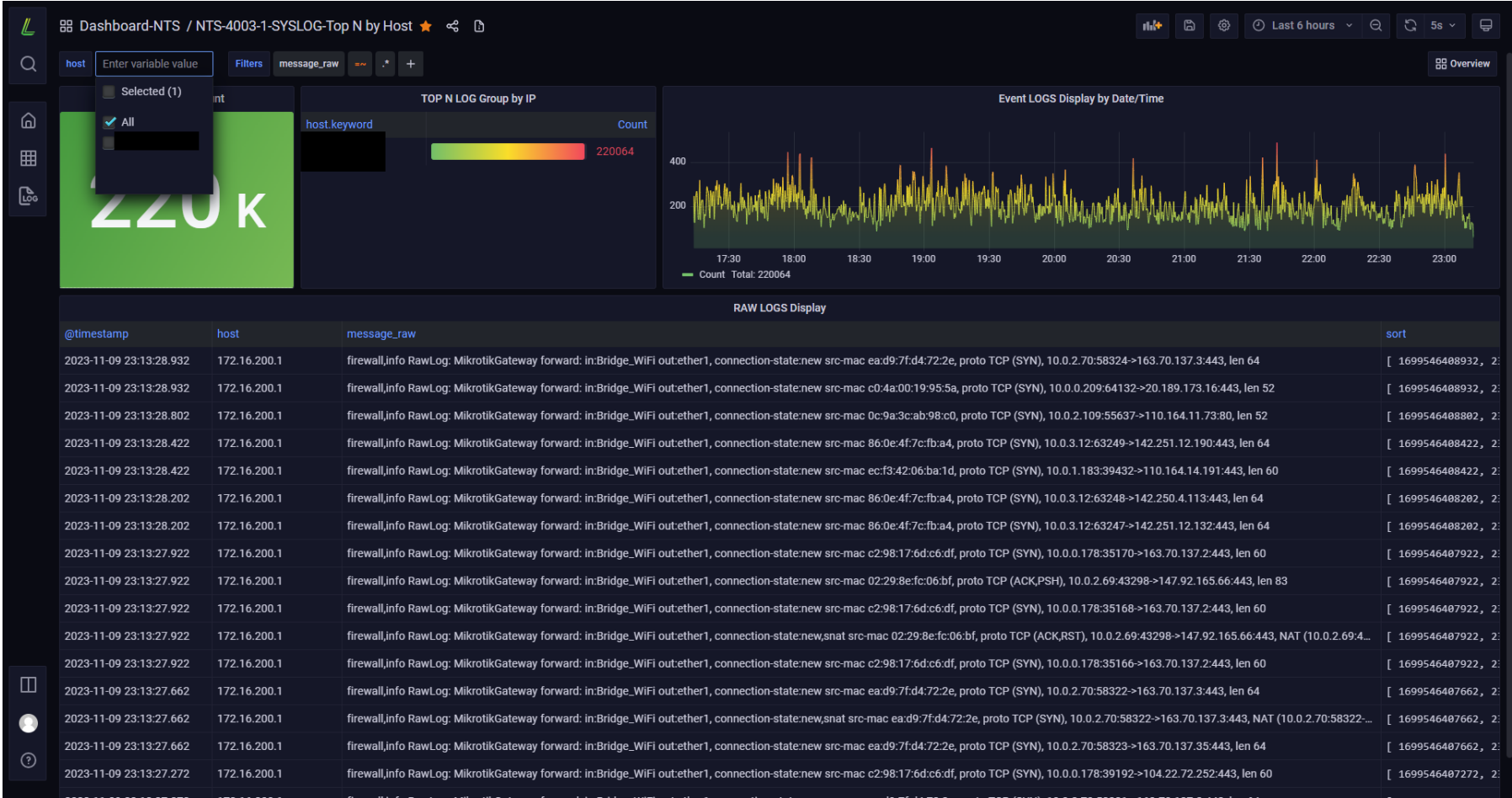


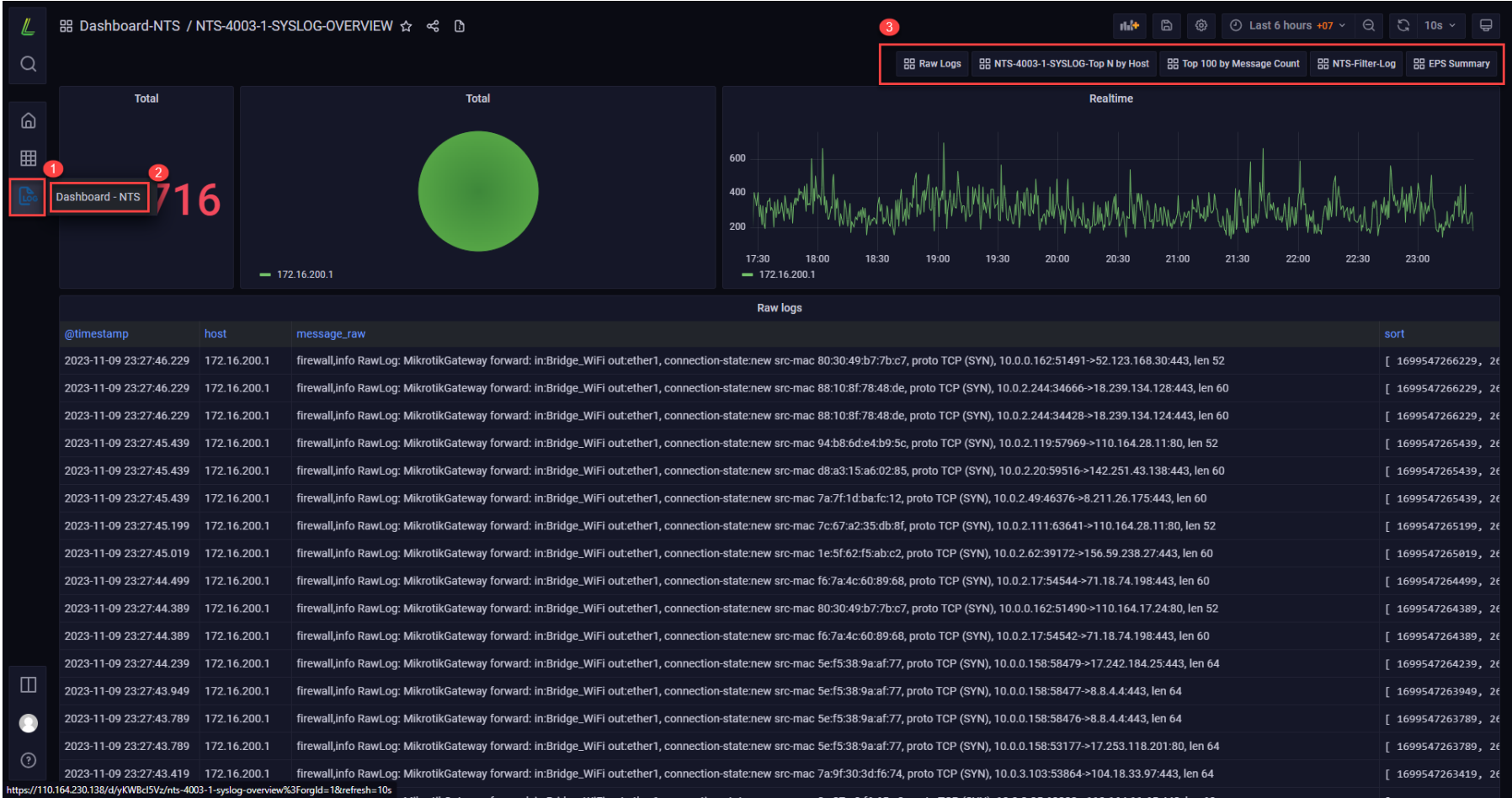
NetkaView Logger

หมายเลข IP และ PORT สำหรับการรับ Log จากอุปกรณ์ไต้หวันทาง



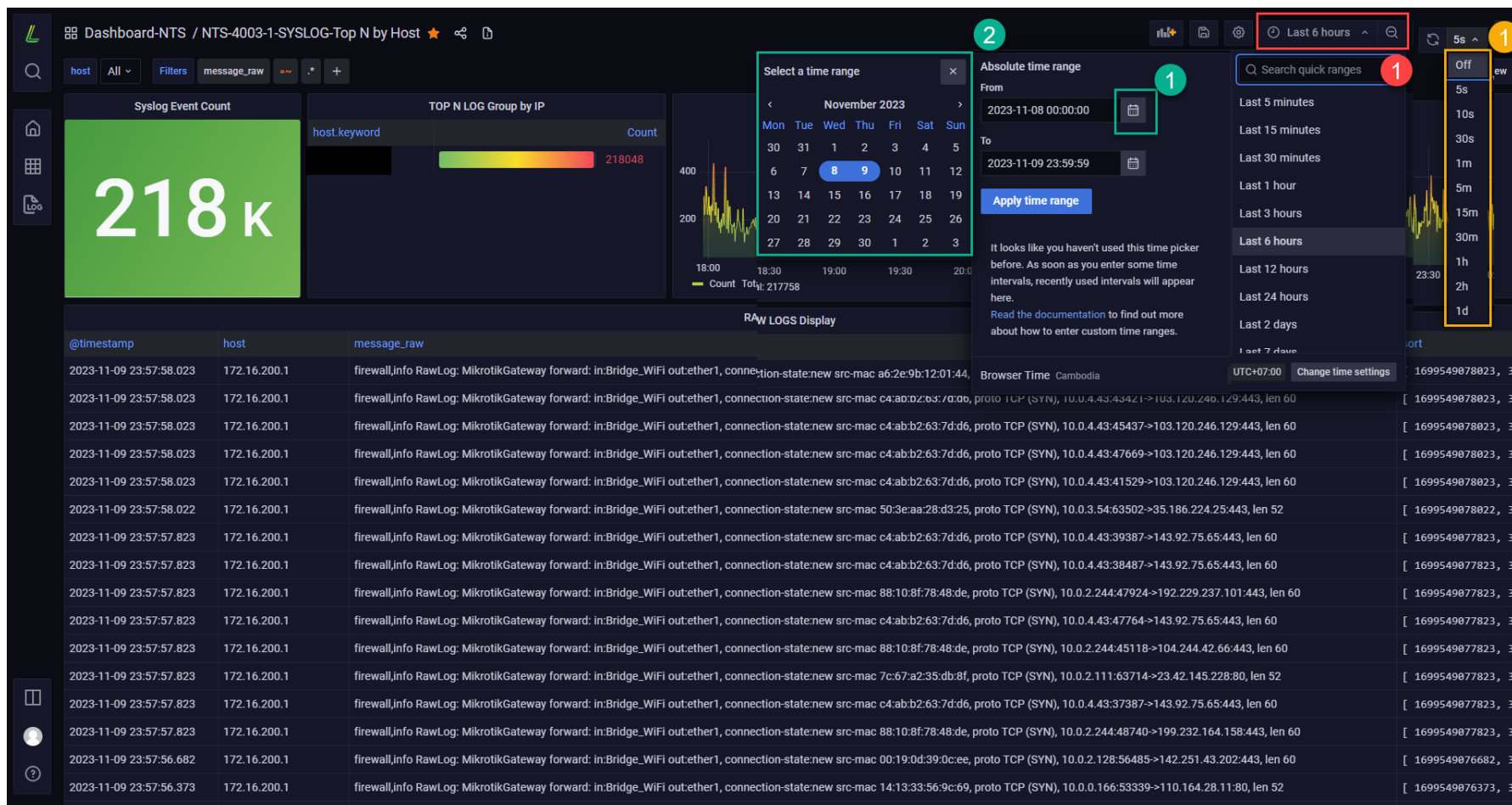
IP	PORT , PROTOCOL
xxx.xxx.xxx.xxx	514/UDP 514/TCP

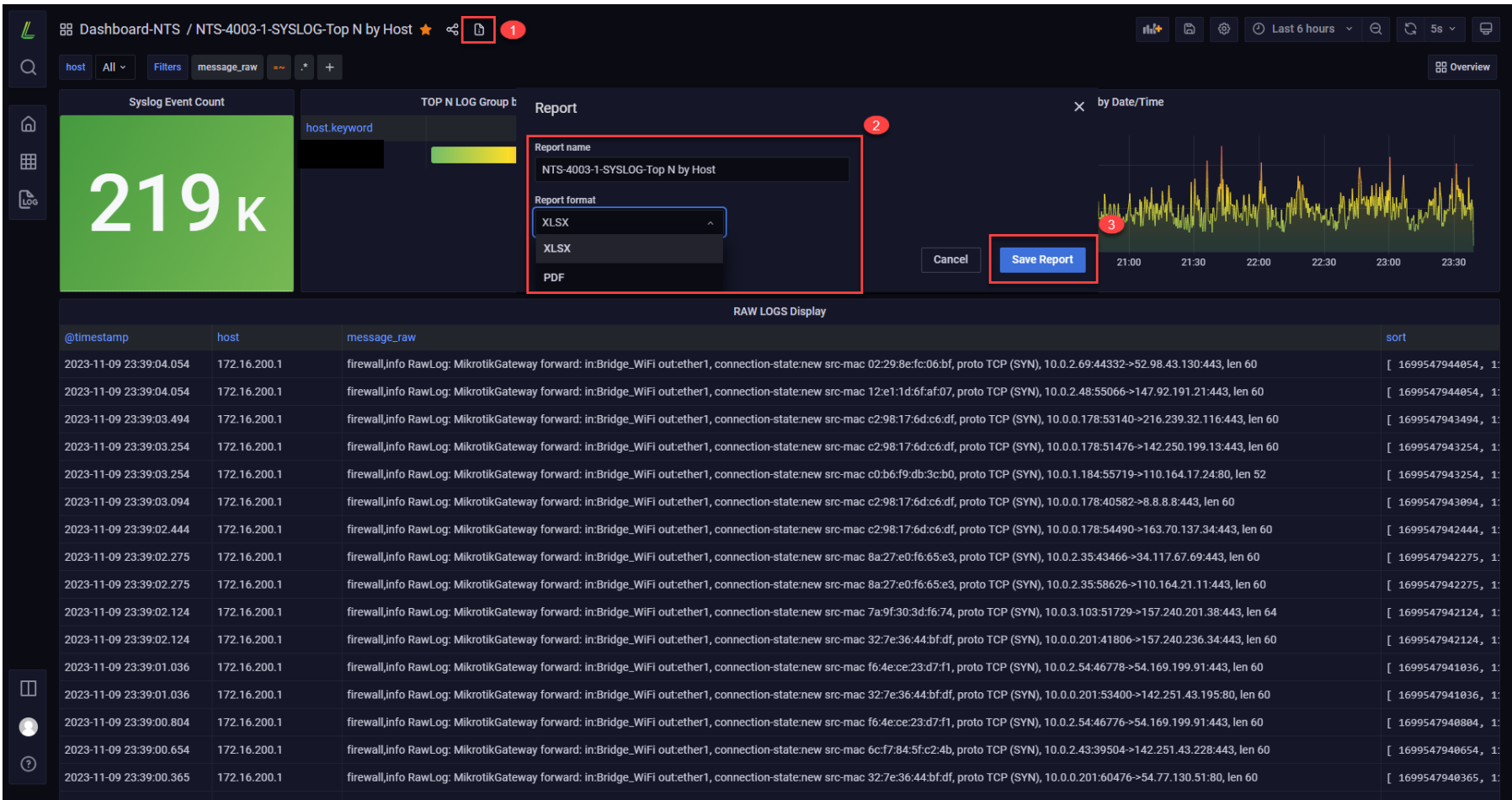


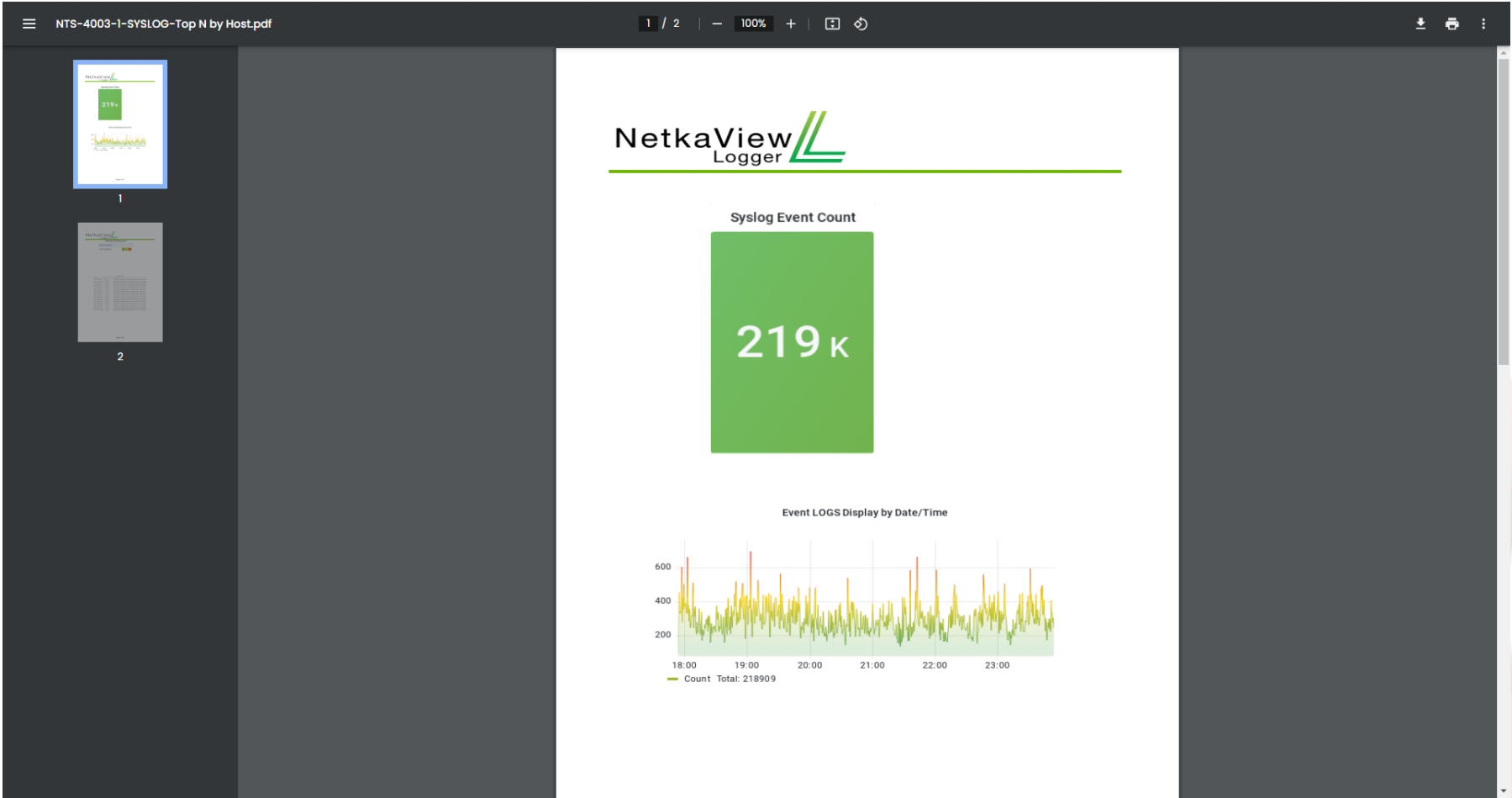


NetkaView Logger

Dashboard Filter Time & Auto Interval Dashboards







NetkaView Logger

Logger Whitelist Management



1

2

3

Logger

Whitelist

Forwarding Log

Logger

Manage your logs

Whitelist

Forwarding Log

Whitelist

Status: Enabled

Disable/Enable: ☒

New whitelist

Hostname	IP Address	Product	Enabled	
Microtik		3Com	☒	x
Portalita		3Com	☒	x

Apply Whitelist

New Whitelist

Hostname

IP Address

Product

3Com

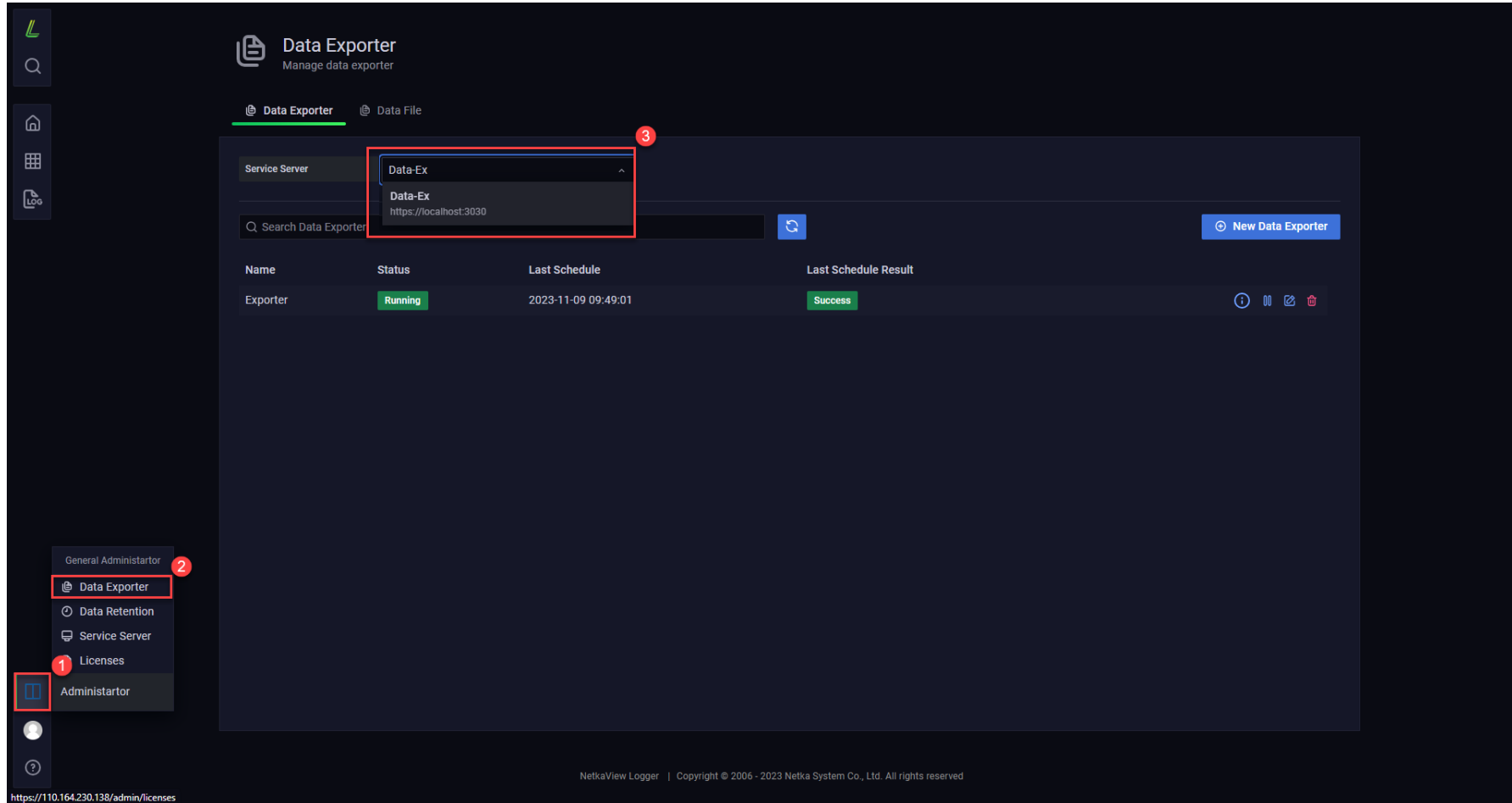
Create whitelist

NetkaView Logger | Copyright © 2006 - 2023 Netka System Co., Ltd. All rights reserved

https://110.164.230.138/admin/whitelist

NetkaView Logger

Data Exporter



NetkaView Logger

Data Exporter Schedule



No	Title	Description
1	Data Export Name	กำหนดชื่อ data exporter
2	Data Source	Data Source Type: กำหนดเป็น elasticsearch Data Source: กำหนดเป็น NLG-SYSLOG
3	Data Configuration	index: กำหนดเป็น logstash-xxx* Time Field: กำหนดเป็น @timestamp Time range: กำหนดระยะที่ต้องการ export log
4	File	Name: กำหนดชื่อไฟล์ที่ต้องการ export log Expiration: ระยะเวลาเก็บ log จากการ export
5	Data Security	เป็นการกำหนด Password , Hashing และ Encryption ข้อมูล
6	Data Export Schedule & Process	เป็นการกำหนดรอบในการ export log interval: เป็นการใส่ช่วงเวลา เช่น 1d,30d เป็นต้น cron: เป็นการกำหนดช่วงเวลาที่จะเรียกมากกว่า interval โดยใช้ crontab เช่น 0 1 * * * หมายถึง ทำการ export log ตอนตี 1 ของทุกวัน

NetkaView Logger

Download Logs from Data Exporter



The screenshot shows the 'Data Exporter' management interface. The left sidebar contains navigation icons and a menu. The main area displays a table of exported data files with columns for Name, Size, From, To, and Expired. Annotations are placed as follows:

- 1: Profile icon in the bottom left sidebar.
- 2: 'Data Exporter' menu item in the left sidebar.
- 3: 'Data File' button at the top of the main area.
- 4: 'Data-Ex' dropdown menu for 'Service Server'.
- 5: 'Exporter' dropdown menu for 'Exporter Service'.
- 6: Action icons (info, refresh, download) for the first row of the data table.

Name	Size	From	To	Expired
Exporter.20231103194800.1.zip	86.8 KiB	2023-11-03 02:48:00	2023-11-04 02:48:00	2024-02-02 02:48:25
Exporter.20231105024900.1.zip	235 KiB	2023-11-04 09:49:00	2023-11-05 09:49:00	2024-02-03 09:49:02
Exporter.20231106024900.1.zip	29.3 KiB	2023-11-05 09:49:00	2023-11-06 09:49:00	2024-02-04 09:49:02
Exporter.20231107024900.1.zip	81.6 KiB	2023-11-06 09:49:00	2023-11-07 09:49:00	2024-02-05 09:49:02
Exporter.20231108024900.1.zip	102 KiB	2023-11-07 09:49:00	2023-11-08 09:49:00	2024-02-06 09:49:02
Exporter.20231109024900.1.zip	3.12 MiB	2023-11-08 09:49:00	2023-11-09 09:49:00	2024-02-07 09:49:10



[illegible]

NetkaView Logger

Export Logs to CSV Files



Dashboard-NTS / NTS-4003-1-SYSLOG-Top N by Host

Syslog Event Count: 137K

TOP N LOG Group by IP: host.keyword Count 137220

Event LOGS Display by Date/Time: 1 queries with total query time of 215 ms

Inspect: RAW LOGS Display

1 Raw logs

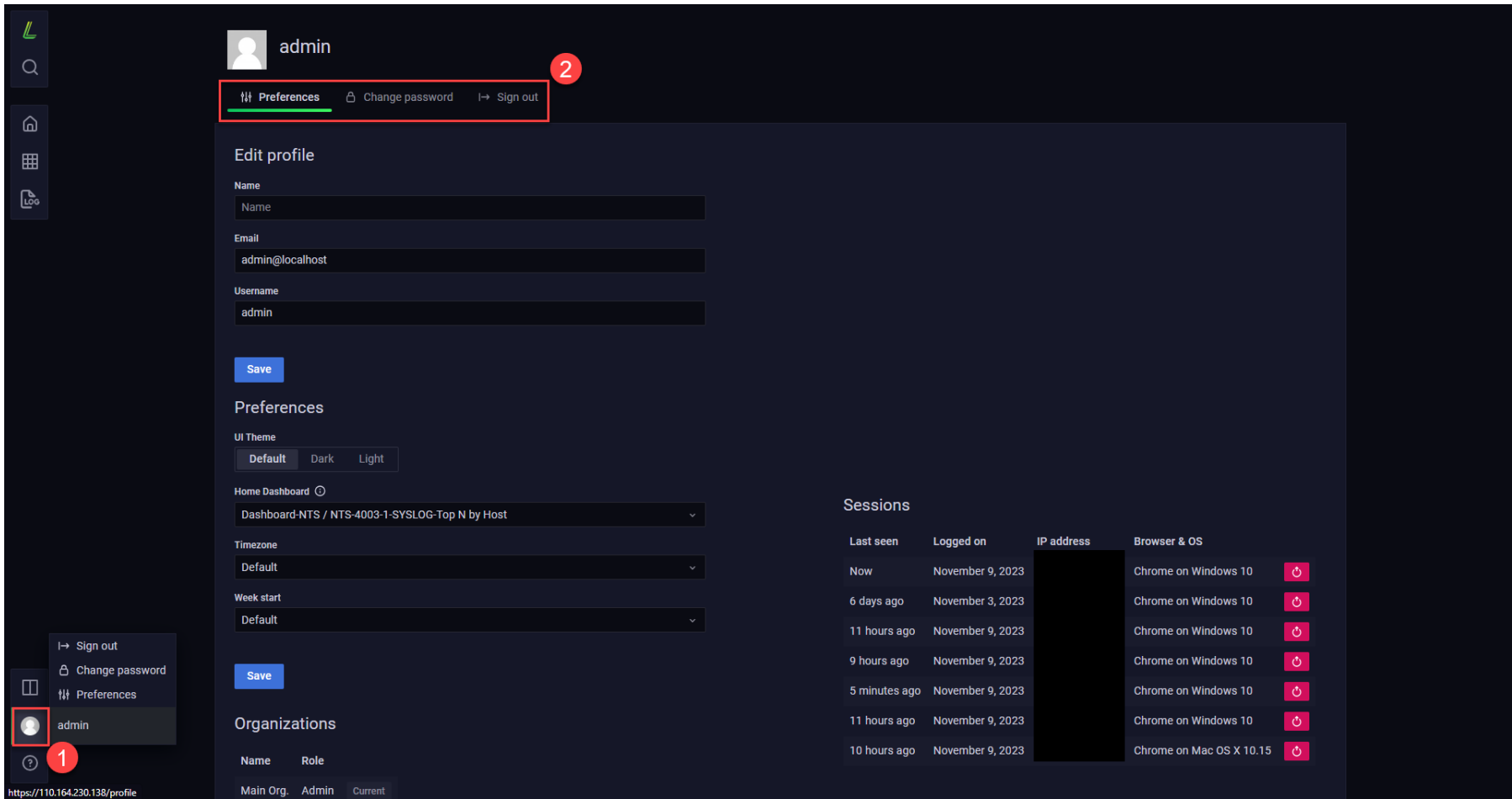
2 Inspect

3 Data

4 Download CSV

5 Download for Excel

@timestamp	host	message_raw
2023-11-10 11:31:49.569	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 42:10:c3:5e:61:3e, proto TCP
2023-11-10 11:31:49.569	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 96:23:07:d7:63:74, proto TCP
2023-11-10 11:31:49.569	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 96:23:07:d7:63:74, proto TCP
2023-11-10 11:31:49.569	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 96:23:07:d7:63:74, proto TCP
2023-11-10 11:31:49.569	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 96:23:07:d7:63:74, proto TCP
2023-11-10 11:31:47.528	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 42:10:c3:5e:61:3e, proto TCP
2023-11-10 11:31:47.318	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 96:23:07:d7:63:74, proto TCP
2023-11-10 11:31:46.998	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac d2:6a:6d:1a:fa:3d, proto TCP
2023-11-10 11:31:46.998	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac d2:6a:6d:1a:fa:3d, proto TCP
2023-11-10 11:31:46.858	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 14:13:33:56:9c:69, proto TCP
2023-11-10 11:31:46.448	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 42:10:c3:5e:61:3e, proto TCP
2023-11-10 11:31:46.148	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 42:10:c3:5e:61:3e, proto TCP
2023-11-10 11:31:45.949	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 42:10:c3:5e:61:3e, proto TCP
2023-11-10 11:31:45.008	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 92:56:c4:6a:d8:d0, proto TCP (SYN), 10.0.2.32:37254->163.70.137.63:443, len 60 [1699590705008, 4]
2023-11-10 11:31:45.008	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac a0:f9:e0:68:d7:8b, proto TCP (SYN), 10.0.2.91:42002->3.94.41.167:443, len 60 [1699590705008, 3]



admin

Preferences Change password Sign out

Edit profile

Name

Email

admin@localhost

Username

admin

Save

Preferences

UI Theme

Default Dark Light

Home Dashboard

Dashboard-NTS / NTS-4003-1-SYSLOG-Top N by Host

Timezone

Default

Week start

Default

Save

Organizations

Name	Role
Main Org.	Admin Current

Sessions

Last seen	Logged on	IP address	Browser & OS
Now	November 9, 2023		Chrome on Windows 10
6 days ago	November 3, 2023		Chrome on Windows 10
11 hours ago	November 9, 2023		Chrome on Windows 10
9 hours ago	November 9, 2023		Chrome on Windows 10
5 minutes ago	November 9, 2023		Chrome on Windows 10
11 hours ago	November 9, 2023		Chrome on Windows 10
10 hours ago	November 9, 2023		Chrome on Mac OS X 10.15

Sign out

Change password

Preferences

admin

https://110.164.230.138/profile

วิธีการ search

search ทุก message ที่เข้ามาในระบบ NLG เป็น default search



Dashboard-NTS / NTS-4003-1-SYSLOG-RAW-DATA ☆ 🔗 📄

Last 6 hours ▾

Host

All ▾

Filters

message_raw

🔍

+

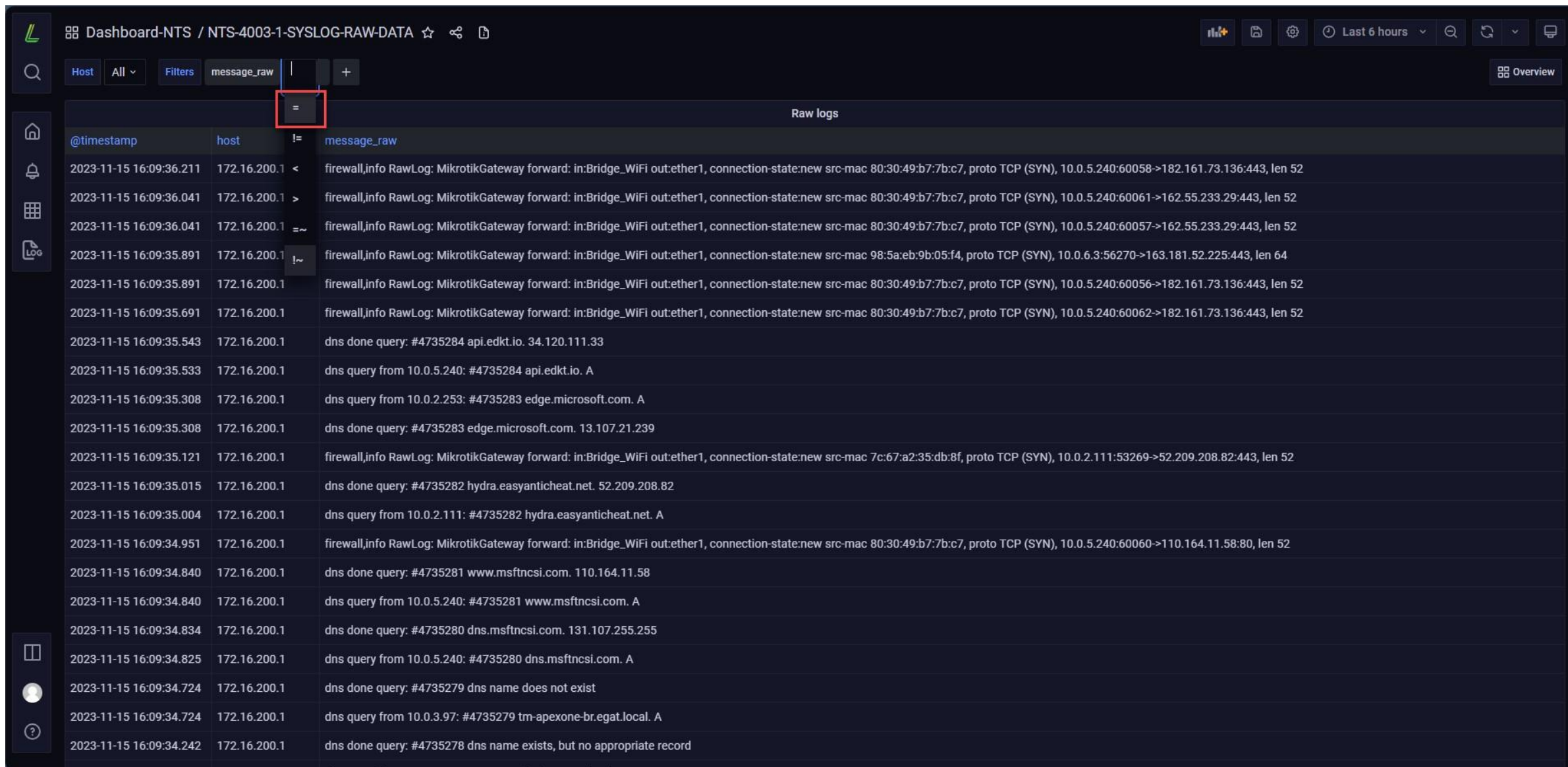
Overview

Raw logs ▾

@timestamp	host	message_raw
2023-11-15 16:09:36.211	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 80:30:49:b7:7b:c7, proto TCP (SYN), 10.0.5.240:60058->182.161.73.136:443, len 52
2023-11-15 16:09:36.041	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 80:30:49:b7:7b:c7, proto TCP (SYN), 10.0.5.240:60061->162.55.233.29:443, len 52
2023-11-15 16:09:36.041	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 80:30:49:b7:7b:c7, proto TCP (SYN), 10.0.5.240:60057->162.55.233.29:443, len 52
2023-11-15 16:09:35.891	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 98:5a:eb:9b:05:f4, proto TCP (SYN), 10.0.6.3:56270->163.181.52.225:443, len 64
2023-11-15 16:09:35.891	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 80:30:49:b7:7b:c7, proto TCP (SYN), 10.0.5.240:60056->182.161.73.136:443, len 52
2023-11-15 16:09:35.691	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 80:30:49:b7:7b:c7, proto TCP (SYN), 10.0.5.240:60062->182.161.73.136:443, len 52
2023-11-15 16:09:35.543	172.16.200.1	dns done query: #4735284 api.edkt.io. 34.120.111.33
2023-11-15 16:09:35.533	172.16.200.1	dns query from 10.0.5.240: #4735284 api.edkt.io. A
2023-11-15 16:09:35.308	172.16.200.1	dns query from 10.0.2.253: #4735283 edge.microsoft.com. A
2023-11-15 16:09:35.308	172.16.200.1	dns done query: #4735283 edge.microsoft.com. 13.107.21.239
2023-11-15 16:09:35.121	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 7c:67:a2:35:db:8f, proto TCP (SYN), 10.0.2.111:53269->52.209.208.82:443, len 52
2023-11-15 16:09:35.015	172.16.200.1	dns done query: #4735282 hydra.easyanticheat.net. 52.209.208.82
2023-11-15 16:09:35.004	172.16.200.1	dns query from 10.0.2.111: #4735282 hydra.easyanticheat.net. A
2023-11-15 16:09:34.951	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 80:30:49:b7:7b:c7, proto TCP (SYN), 10.0.5.240:60060->110.164.11.58:80, len 52
2023-11-15 16:09:34.840	172.16.200.1	dns done query: #4735281 www.msftncsi.com. 110.164.11.58
2023-11-15 16:09:34.840	172.16.200.1	dns query from 10.0.5.240: #4735281 www.msftncsi.com. A
2023-11-15 16:09:34.834	172.16.200.1	dns done query: #4735280 dns.msftncsi.com. 131.107.255.255
2023-11-15 16:09:34.825	172.16.200.1	dns query from 10.0.5.240: #4735280 dns.msftncsi.com. A
2023-11-15 16:09:34.724	172.16.200.1	dns done query: #4735279 dns name does not exist
2023-11-15 16:09:34.724	172.16.200.1	dns query from 10.0.3.97: #4735279 tm-apexone-br.egat.local. A
2023-11-15 16:09:34.242	172.16.200.1	dns done query: #4735278 dns name exists, but no appropriate record
2023-11-15 16:09:34.232	172.16.200.1	dns query from 10.0.2.253: #4735278 login.supercloud2.com. AAAA

วิธีการ search

เปลี่ยนเงื่อนไข เป็น =



The screenshot shows the Netka dashboard interface. At the top, the breadcrumb navigation reads "Dashboard-NTS / NTS-4003-1-SYSLOG-RAW-DATA". Below this, there are tabs for "Host", "All", "Filters", and "message_raw". A search bar contains the text "message_raw" followed by a filter icon and a plus sign. A red box highlights the filter icon, which currently shows "!=". The main area displays a table of raw logs. The table has columns for "@timestamp", "host", and "message_raw". The logs show various firewall and DNS events. On the left sidebar, there are icons for home, notifications, a grid, and a document labeled "Log". On the right sidebar, there are icons for a bar chart, a document, a gear, a clock set to "Last 6 hours", a search icon, a refresh icon, and a dropdown menu. An "Overview" button is also present in the top right corner.

@timestamp	host	message_raw
2023-11-15 16:09:36.211	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 80:30:49:b7:7b:c7, proto TCP (SYN), 10.0.5.240:60058->182.161.73.136:443, len 52
2023-11-15 16:09:36.041	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 80:30:49:b7:7b:c7, proto TCP (SYN), 10.0.5.240:60061->162.55.233.29:443, len 52
2023-11-15 16:09:36.041	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 80:30:49:b7:7b:c7, proto TCP (SYN), 10.0.5.240:60057->162.55.233.29:443, len 52
2023-11-15 16:09:35.891	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 98:5a:eb:9b:05:f4, proto TCP (SYN), 10.0.6.3:56270->163.181.52.225:443, len 64
2023-11-15 16:09:35.891	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 80:30:49:b7:7b:c7, proto TCP (SYN), 10.0.5.240:60056->182.161.73.136:443, len 52
2023-11-15 16:09:35.691	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 80:30:49:b7:7b:c7, proto TCP (SYN), 10.0.5.240:60062->182.161.73.136:443, len 52
2023-11-15 16:09:35.543	172.16.200.1	dns done query: #4735284 api.edkt.io. 34.120.111.33
2023-11-15 16:09:35.533	172.16.200.1	dns query from 10.0.5.240: #4735284 api.edkt.io. A
2023-11-15 16:09:35.308	172.16.200.1	dns query from 10.0.2.253: #4735283 edge.microsoft.com. A
2023-11-15 16:09:35.308	172.16.200.1	dns done query: #4735283 edge.microsoft.com. 13.107.21.239
2023-11-15 16:09:35.121	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 7c:67:a2:35:db:8f, proto TCP (SYN), 10.0.2.111:53269->52.209.208.82:443, len 52
2023-11-15 16:09:35.015	172.16.200.1	dns done query: #4735282 hydra.easyanticheat.net. 52.209.208.82
2023-11-15 16:09:35.004	172.16.200.1	dns query from 10.0.2.111: #4735282 hydra.easyanticheat.net. A
2023-11-15 16:09:34.951	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 80:30:49:b7:7b:c7, proto TCP (SYN), 10.0.5.240:60060->110.164.11.58:80, len 52
2023-11-15 16:09:34.840	172.16.200.1	dns done query: #4735281 www.msftncsi.com. 110.164.11.58
2023-11-15 16:09:34.840	172.16.200.1	dns query from 10.0.5.240: #4735281 www.msftncsi.com. A
2023-11-15 16:09:34.834	172.16.200.1	dns done query: #4735280 dns.msftncsi.com. 131.107.255.255
2023-11-15 16:09:34.825	172.16.200.1	dns query from 10.0.5.240: #4735280 dns.msftncsi.com. A
2023-11-15 16:09:34.724	172.16.200.1	dns done query: #4735279 dns name does not exist
2023-11-15 16:09:34.724	172.16.200.1	dns query from 10.0.3.97: #4735279 tm-apexone-br.egat.local. A
2023-11-15 16:09:34.242	172.16.200.1	dns done query: #4735278 dns name exists, but no appropriate record

วิธีการ search

ใส่คำที่ต้องการ search

Dashboard-NTS / NTS-4003-1-SYSLOG-RAW-DATA ☆ 🔊 📄

Host

All

Filters

message_raw

OPPO

+

Overview

Raw logs

@timestamp	host	message_raw
2023-11-15 16:09:56.182	172.16.200.1	dhcp,info DHCP_WiFi deassigned 10.0.7.48 for 00:08:22:40:EE 88 OPPO-A31
2023-11-15 16:07:07.487	172.16.200.1	dhcp,info DHCP_WiFi assigned 10.0.5.206 for 22:8D:38:62:F3:2A OPPO-A96
2023-11-15 16:07:04.501	172.16.200.1	dhcp,info DHCP_WiFi deassigned 10.0.5.206 for 22:8D:38:62:F3:2A OPPO-A96
2023-11-15 16:05:40.393	172.16.200.1	dhcp,info DHCP_WiFi assigned 10.0.5.208 for 86:96:C2:65:4E:0D OPPO-A96
2023-11-15 16:05:05.988	172.16.200.1	dhcp,info DHCP_WiFi assigned 10.0.2.59 for B6:D9:33:6D:A0:B3 OPPO-Reno5-5G
2023-11-15 16:02:29.624	172.16.200.1	dhcp,info DHCP_WiFi assigned 10.0.2.85 for 0E:27:DB:0A:86:5C OPPO-A15
2023-11-15 16:02:18.099	172.16.200.1	dhcp,info DHCP_WiFi deassigned 10.0.2.85 for 0E:27:DB:0A:86:5C OPPO-A15
2023-11-15 16:00:58.419	172.16.200.1	dhcp,info DHCP_WiFi assigned 10.0.5.175 for 96:C2:BC:66:4F:2A OPPO-Reno7-Z-5G
2023-11-15 16:00:58.396	172.16.200.1	dhcp,info DHCP_WiFi deassigned 10.0.5.175 for 96:C2:BC:66:4F:2A OPPO-Reno7-Z-5G
2023-11-15 16:00:47.388	172.16.200.1	dhcp,info DHCP_WiFi assigned 10.0.0.212 for A4:F0:5E:E0:47:0F OPPO-A5s
2023-11-15 16:00:47.324	172.16.200.1	dhcp,info DHCP_WiFi deassigned 10.0.0.212 for A4:F0:5E:E0:47:0F OPPO-A5s
2023-11-15 15:59:43.119	172.16.200.1	dhcp,info DHCP_WiFi assigned 10.0.7.76 for D4:67:D3:37:60:7D OPPO-A3s
2023-11-15 15:58:54.965	172.16.200.1	dhcp,info DHCP_WiFi deassigned 10.0.7.39 for 5E:66:77:89:81:34 OPPO-A95
2023-11-15 15:58:46.219	172.16.200.1	dhcp,info DHCP_WiFi assigned 10.0.5.175 for 96:C2:BC:66:4F:2A OPPO-Reno7-Z-5G
2023-11-15 15:58:46.206	172.16.200.1	dhcp,info DHCP_WiFi deassigned 10.0.5.175 for 96:C2:BC:66:4F:2A OPPO-Reno7-Z-5G
2023-11-15 15:58:11.036	172.16.200.1	dhcp,info DHCP_WiFi deassigned 10.0.5.208 for 86:96:C2:65:4E:0D OPPO-A96
2023-11-15 15:57:56.540	172.16.200.1	dhcp,info DHCP_WiFi assigned 10.0.5.175 for 96:C2:BC:66:4F:2A OPPO-Reno7-Z-5G
2023-11-15 15:57:56.524	172.16.200.1	dhcp,info DHCP_WiFi deassigned 10.0.5.175 for 96:C2:BC:66:4F:2A OPPO-Reno7-Z-5G
2023-11-15 15:57:24.431	172.16.200.1	dhcp,info DHCP_WiFi deassigned 10.0.2.59 for B6:D9:33:6D:A0:B3 OPPO-Reno5-5G
2023-11-15 15:55:12.557	172.16.200.1	dhcp,info DHCP_WiFi assigned 10.0.2.59 for B6:D9:33:6D:A0:B3 OPPO-Reno5-5G
2023-11-15 15:55:12.529	172.16.200.1	dhcp,info DHCP_WiFi deassigned 10.0.2.59 for B6:D9:33:6D:A0:B3 OPPO-Reno5-5G
2023-11-15 15:51:40.075	172.16.200.1	dhcp,info DHCP_WiFi assigned 10.0.5.208 for 86:96:C2:65:4E:0D OPPO-A96