NetkaView Logger
Netka System

อุปกรณ์เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

NetkaView Logger | NLG-SW | บริษัท เน็ตก้า ซิสเต็ม จำกัด

ได้รับการรับรองตามมาตรฐาน มศอ. 4003.1-2560

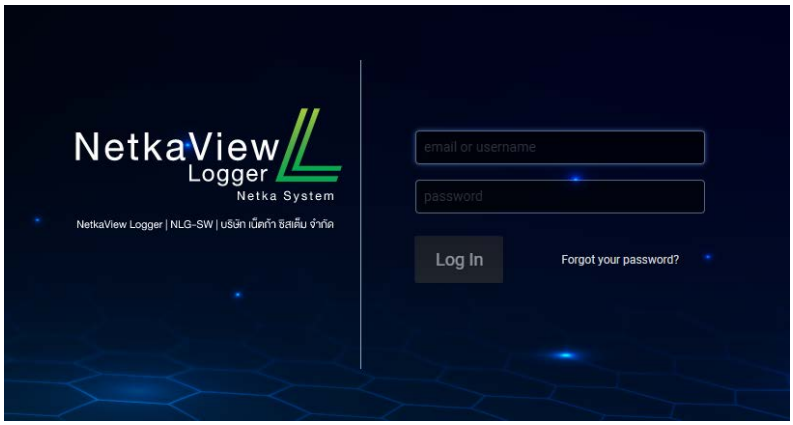
จุดเด่นของผลิตภัณฑ์

- 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 มศอ.4003.1-2560 “ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์” โดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ซึ่งเป็นข้อกำหนดที่ถูกพัฒนาโดยอ้างอิงพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

NetkaView Logger สามารถรับ เก็บบันทึก และรักษาบูรณภาพข้อมูลจราจรทางคอมพิวเตอร์ตามหลักการที่ถูกต้องโดยชอบด้วยกฎหมาย เพื่อลดความเสี่ยงต่อการสูญเสียความถูกต้องสมบูรณ์ของข้อมูล (Data Integrity) และเพียงพอสำหรับระบุผู้เกี่ยวข้องได้อย่างน่าเชื่อถือ



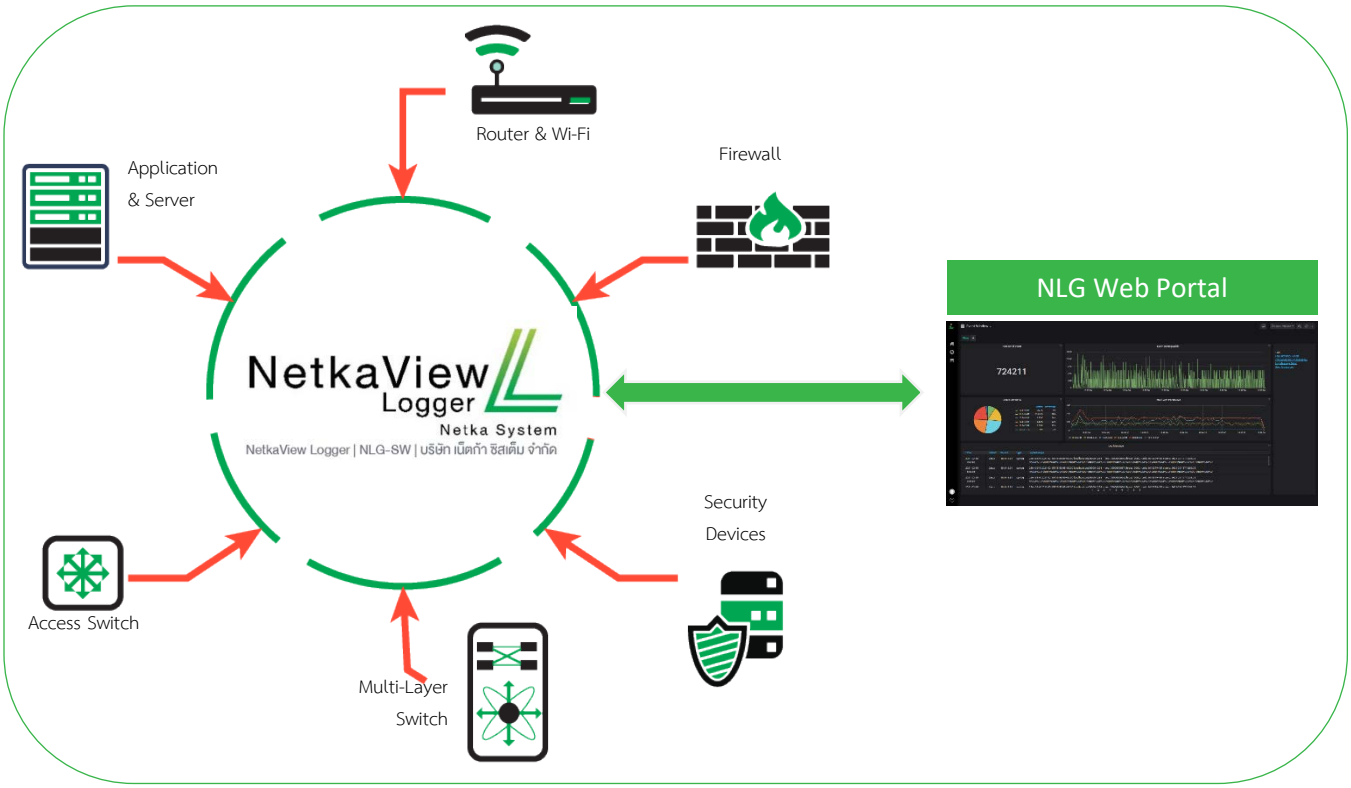
คุณสมบัติของผลิตภัณฑ์ NLG

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 มศอ.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

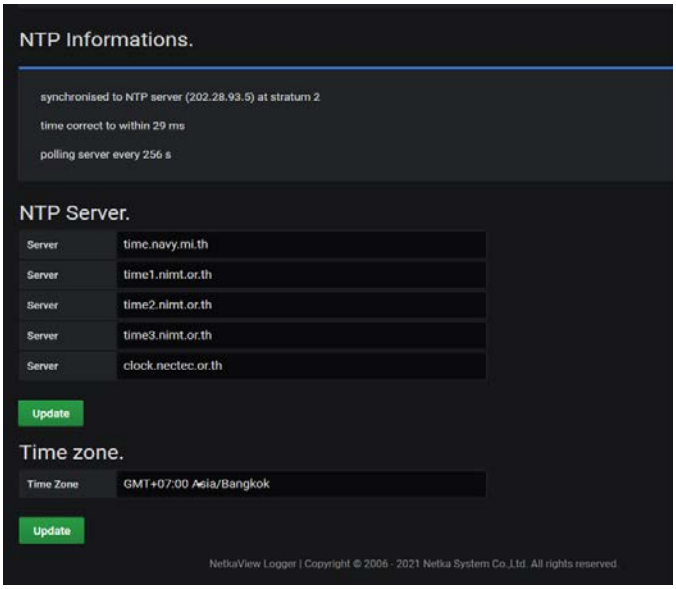
การติดตั้งระบบ NLG ภายในเครือข่ายคอมพิวเตอร์เพื่อเก็บบันทึกการทำงาน (Log) ให้กับระบบสารสนเทศซึ่งประกอบด้วยอุปกรณ์เครือข่าย เครื่องแม่ข่าย ระบบงาน อุปกรณ์รักษาความปลอดภัย และอุปกรณ์ด้านสารสนเทศอื่นๆ

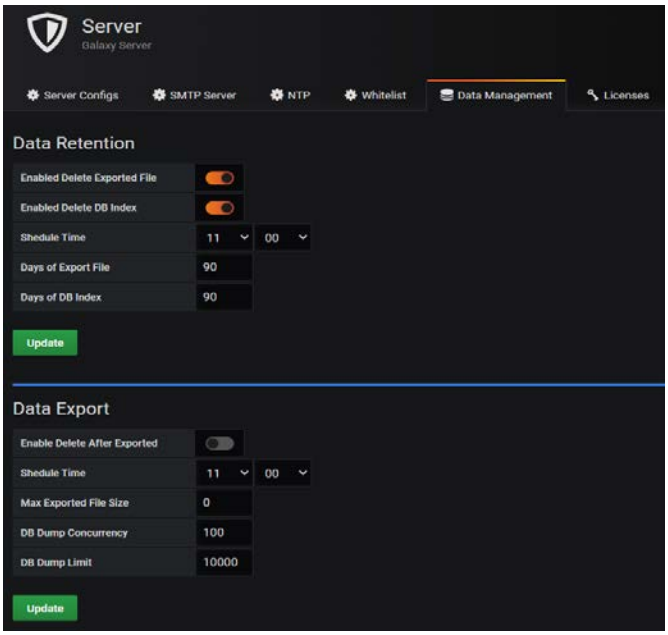


คุณสมบัติของผลิตภัณฑ์ NLG

Network Time Protocol (NTP)

มีคุณสมบัติในการตั้งค่า Network Time Protocol (NTP) และค่าเวลา Time zone ซึ่งใช้สำหรับการกำหนดเวลามาตรฐาน เพื่อตั้งค่าเวลาของระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ให้ตรงกับเวลามาตรฐานสากล



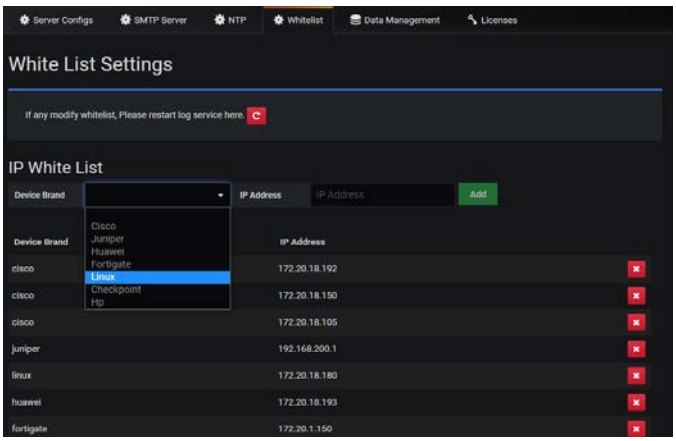


Data Management

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

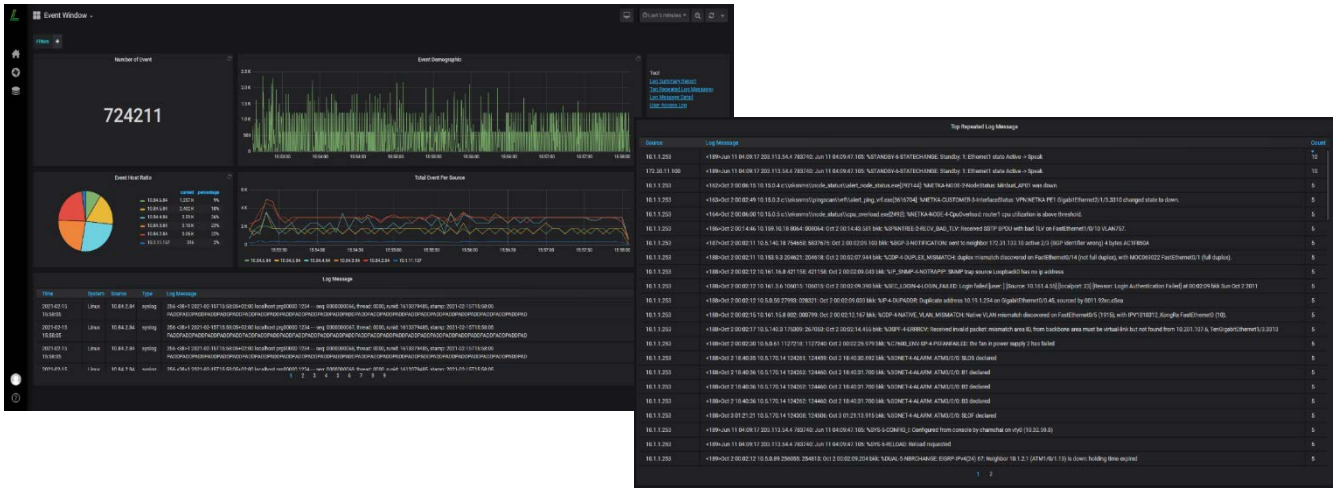
Whitelist / Filtering

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 เวอร์ชั่น 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

ซึ่งได้ผ่านการตรวจสอบแล้วพบว่ามีคุณภาพเป็นไปตามหลักเกณฑ์และเงื่อนไขการรับรองคุณภาพผลิตภัณฑ์ของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ และเป็นไปตามข้อกำหนดของมาตรฐานดังนี้

มศอ. 4003.1-2560 ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ เล่ม 1 ข้อกำหนด

ภายใต้ขอบข่ายผลิตภัณฑ์ที่ระบุข้างต้น บริษัทฯ สามารถนำใบรับรอง และเครื่องหมายรับรองคุณภาพผลิตภัณฑ์ ของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ไปใช้ได้ **โดยต้อง** ปฏิบัติตามหลักเกณฑ์และเงื่อนไขการใช้ใบรับรอง ทั้งนี้ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ จะดำเนินการตรวจสอบและควบคุมคุณภาพผลิตภัณฑ์ที่ได้รับการรับรองนี้ 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

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
112 อุทยานวิทยาศาสตร์ประเทศไทย ถนนพหลโยธิน ตำบลคลองหนึ่ง อำเภอคลองหลวง
จังหวัดปทุมธานี 12120 โทรศัพท์ 0 2564 6900 โทรสาร 0 2564 6889

National Electronics and Computer Technology Center
National Science and Technology Development Agency
112 Thailand Science Park, Phahonyothin Road, Klong 1, Klong Luang,
Pathumthani 12120, Thailand. Tel. +66 254 6900 Fax. +66 2564 6889

NLG มศอ. 4003.1-2560 (Centralized Log)

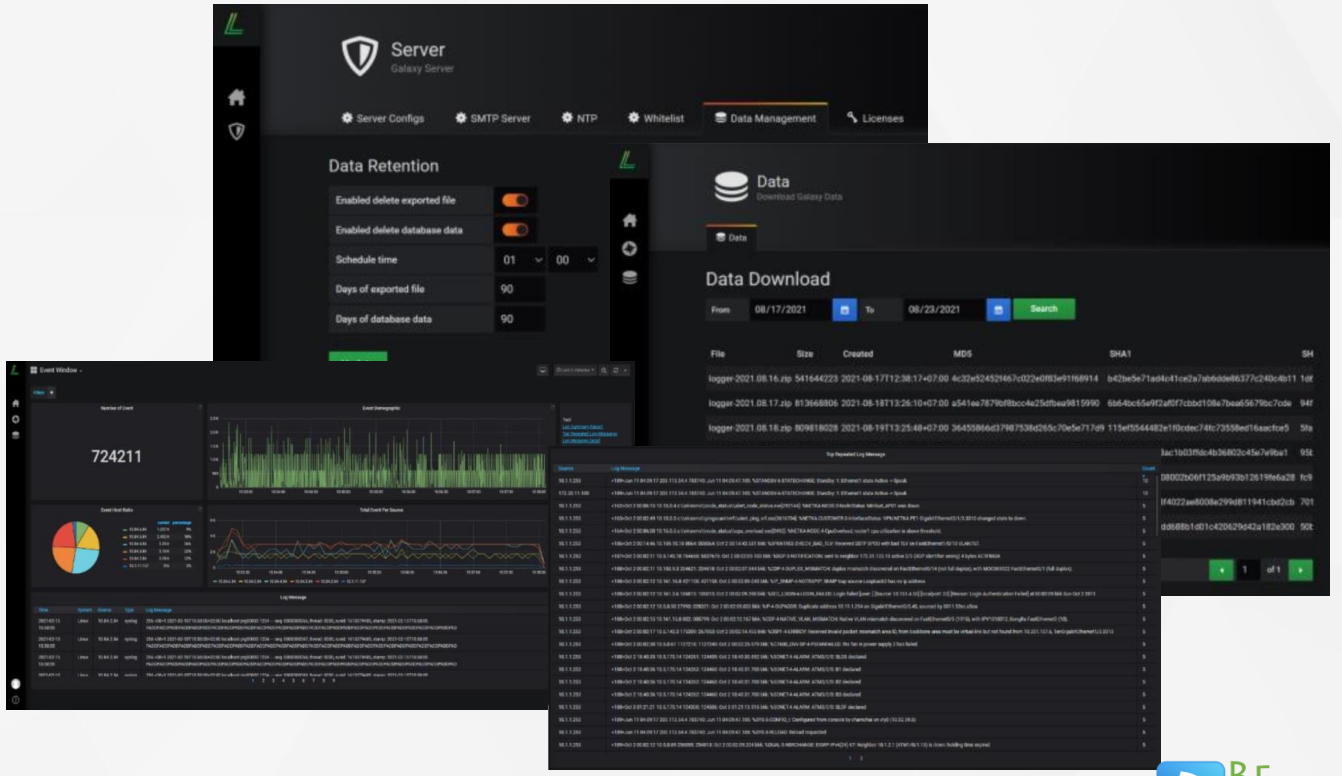
NetkaView Logger

NetkaView Logger(NLG) มศอ. 4003.1-2560

เป็นอุปกรณ์เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผ่านการทดสอบและ ได้รับการรับรองตามข้อกำหนดของมาตรฐาน มศอ.4003.1-2560 “ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์” โดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และ คอมพิวเตอร์แห่งชาติ ซึ่งเป็นข้อกำหนดที่ถูกพัฒนาโดยอ้างอิงพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

Key Features & Product Highlights:

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



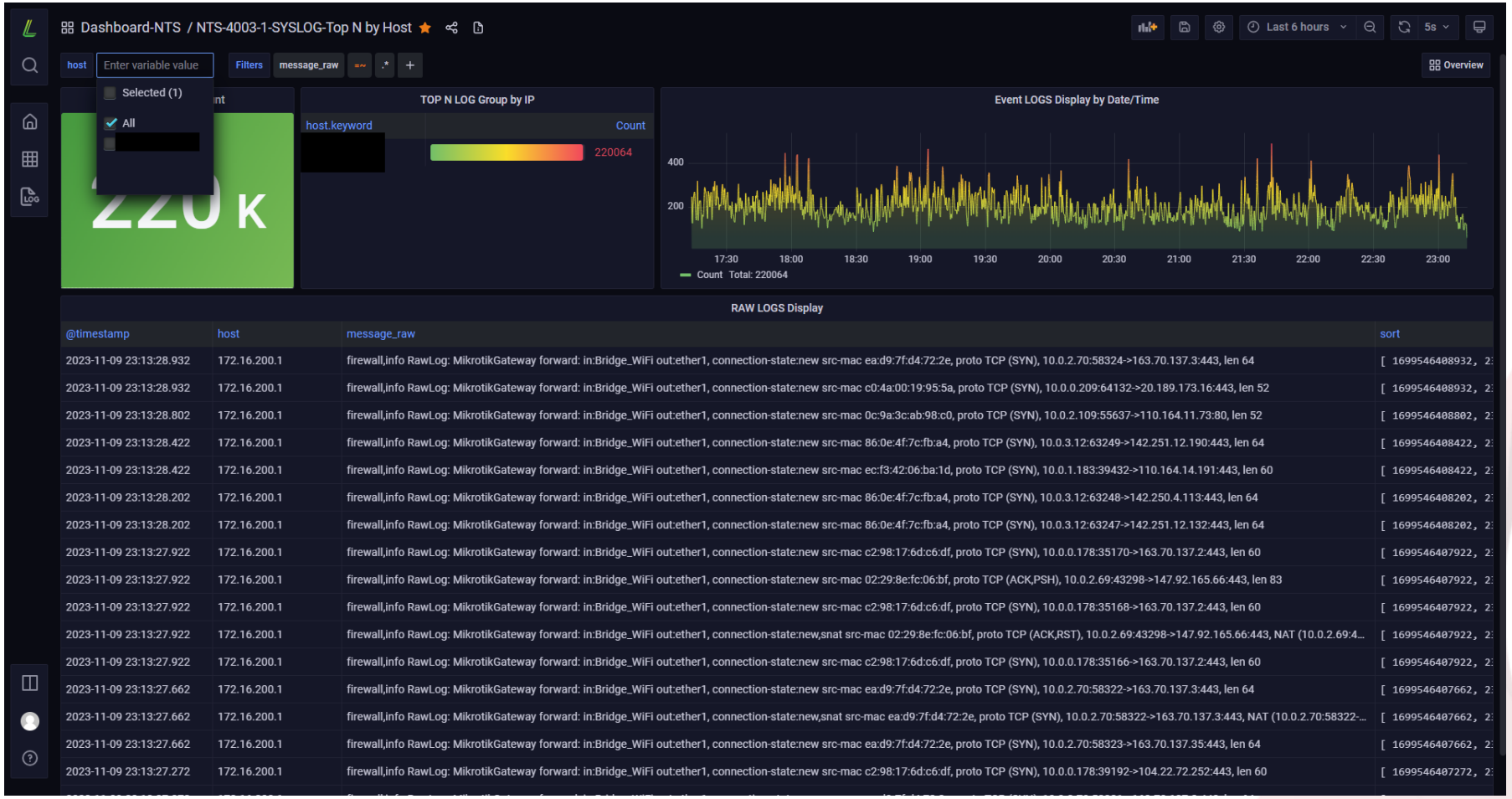
NetkaView Logger

หมายเลข IP และ PORT สำหรับการรับ Log จากอุปกรณ์ต้นทาง

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

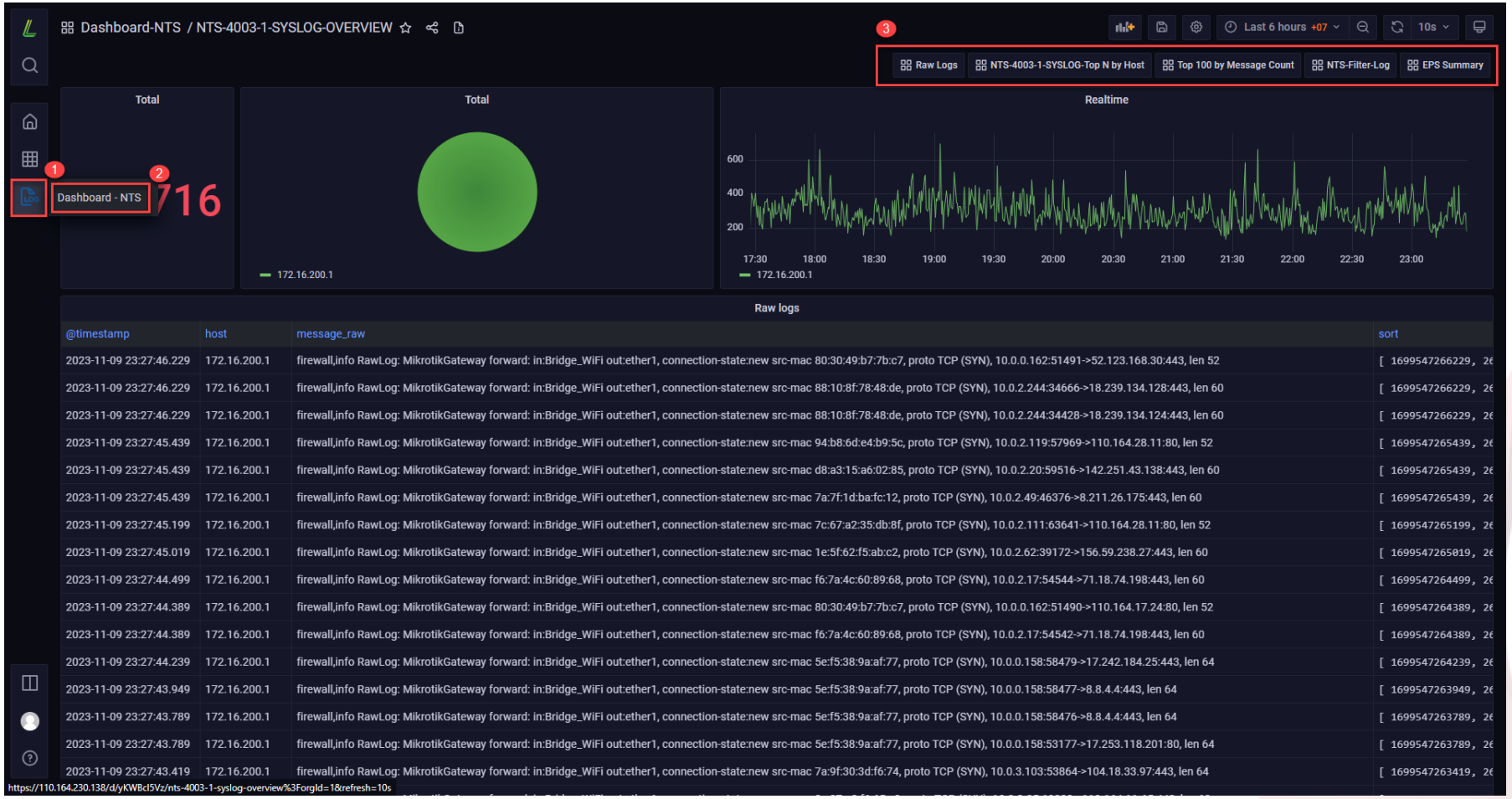
NetkaView Logger

Home Page



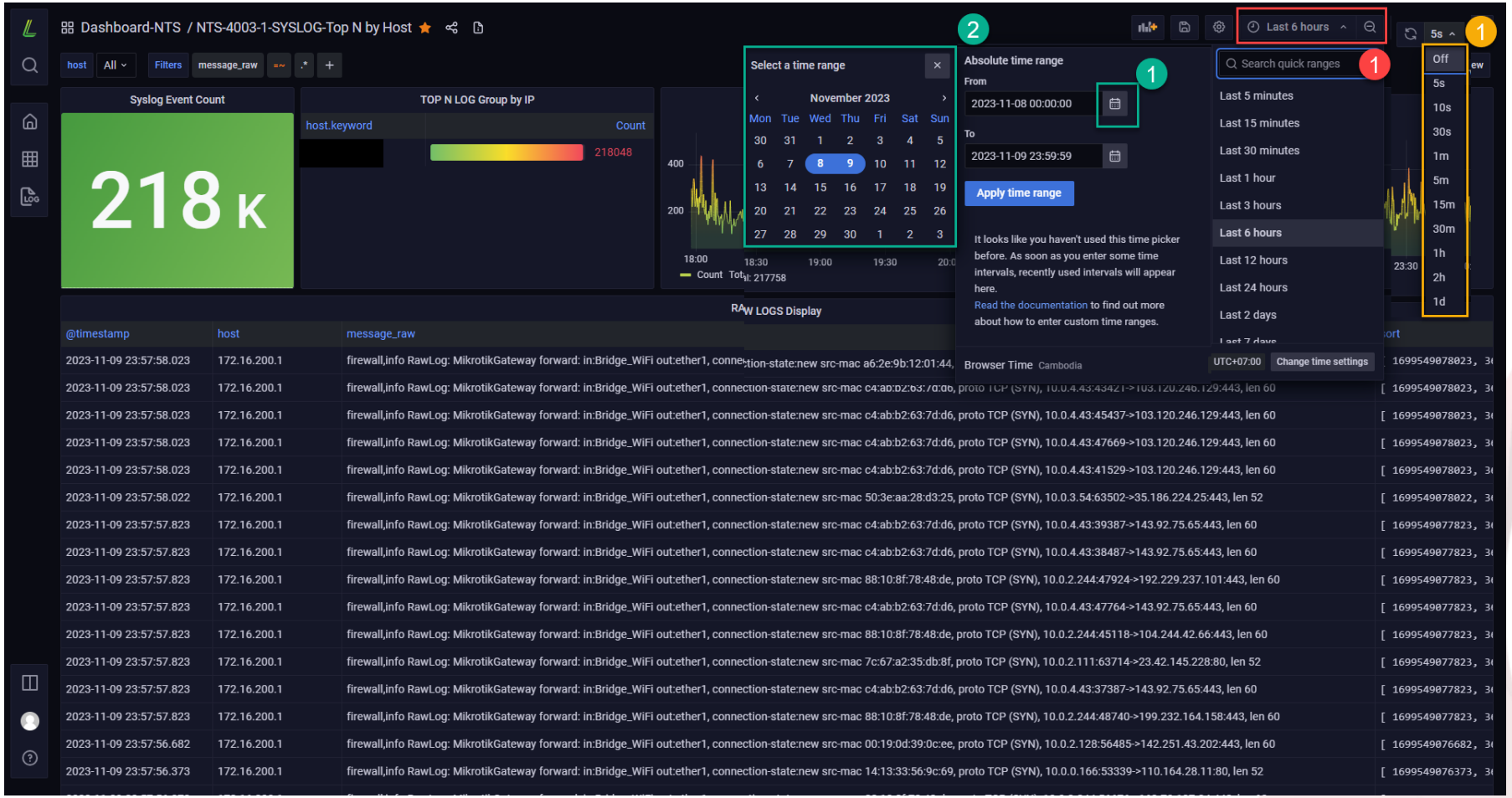
NetkaView Logger

Menu Dashboard - NTS



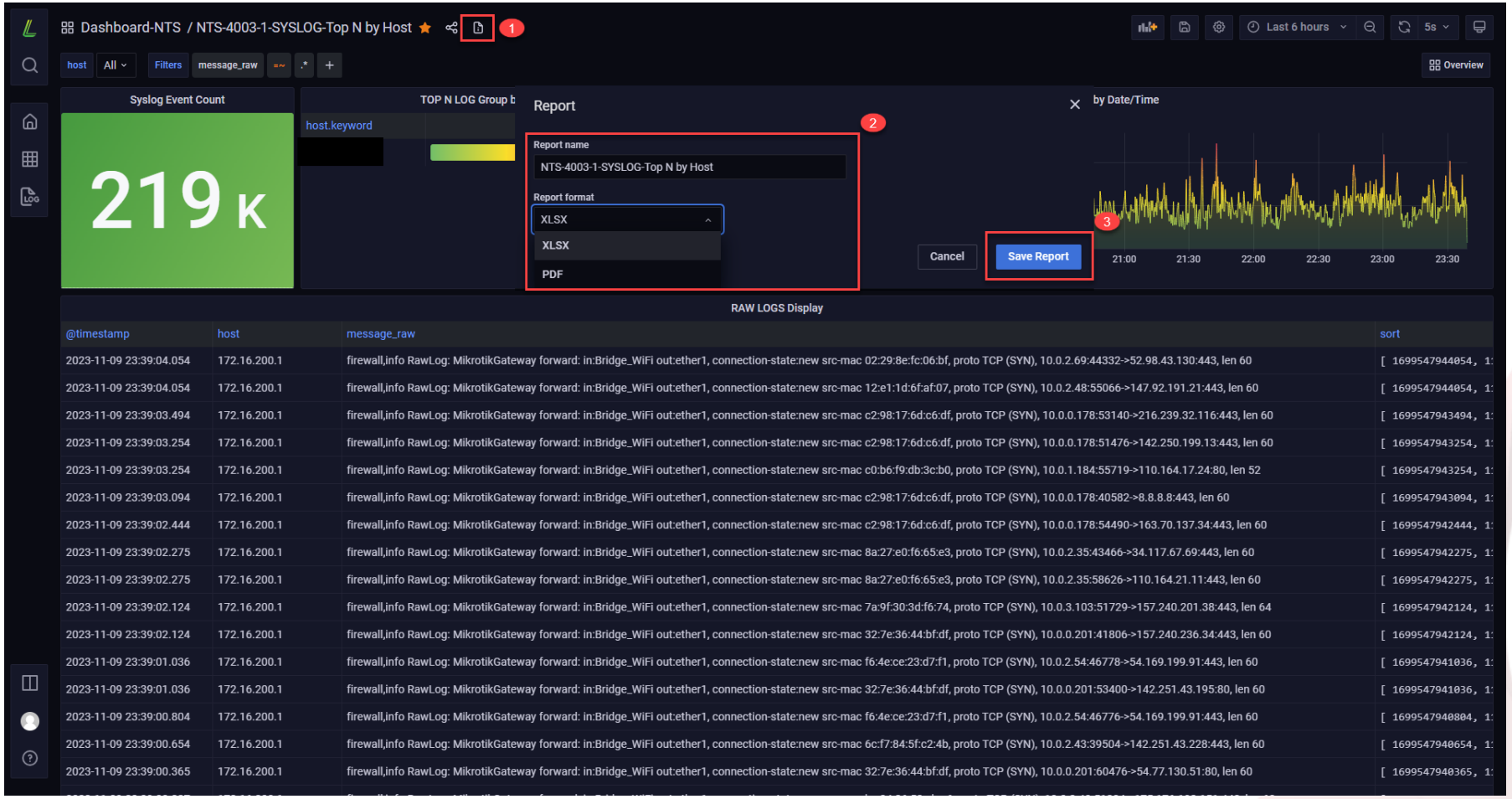
NetkaView Logger

Dashboard Filter Time & Auto Interval Dashboards



NetkaView Logger

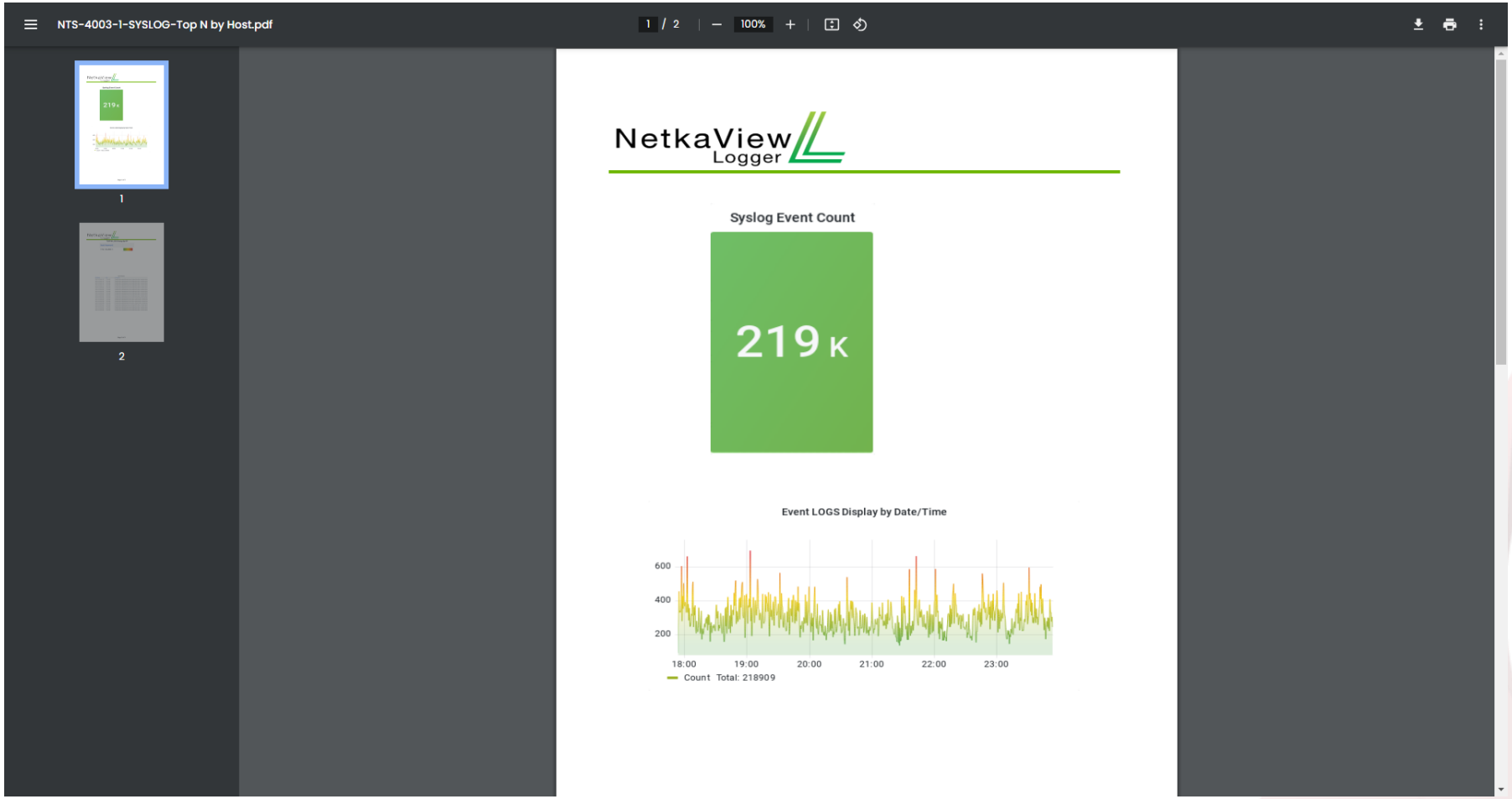
Report Dashboard



@timestamp	host	message_raw	sort
2023-11-09 23:39:04.054	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 02:29:8e:fc:06:bf, proto TCP (SYN), 10.0.2.69:44332->52.98.43.130:443, len 60	[1699547944054, 1
2023-11-09 23:39:04.054	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 12:e1:1d:6f:af:07, proto TCP (SYN), 10.0.2.48:55066->147.92.191.21:443, len 60	[1699547944054, 1
2023-11-09 23:39:03.494	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac c2:98:17:6d:c6:df, proto TCP (SYN), 10.0.0.178:53140->216.239.32.116:443, len 60	[1699547943494, 1
2023-11-09 23:39:03.254	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac c2:98:17:6d:c6:df, proto TCP (SYN), 10.0.0.178:51476->142.250.199.13:443, len 60	[1699547943254, 1
2023-11-09 23:39:03.254	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac c0:b6:f9:db:3c:b0, proto TCP (SYN), 10.0.1.184:55719->110.164.17.24:80, len 52	[1699547943254, 1
2023-11-09 23:39:03.094	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac c2:98:17:6d:c6:df, proto TCP (SYN), 10.0.0.178:40582->8.8.8.8:443, len 60	[1699547943094, 1
2023-11-09 23:39:02.444	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac c2:98:17:6d:c6:df, proto TCP (SYN), 10.0.0.178:54490->163.70.137.34:443, len 60	[1699547942444, 1
2023-11-09 23:39:02.275	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 8a:27:e0:f6:65:e3, proto TCP (SYN), 10.0.2.35:43466->34.117.67.69:443, len 60	[1699547942275, 1
2023-11-09 23:39:02.275	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 8a:27:e0:f6:65:e3, proto TCP (SYN), 10.0.2.35:58626->110.164.21.11:443, len 60	[1699547942275, 1
2023-11-09 23:39:02.124	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 7a:9f:30:3d:f6:74, proto TCP (SYN), 10.0.3.103:51729->157.240.201.38:443, len 64	[1699547942124, 1
2023-11-09 23:39:02.124	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 32:7e:36:44:bf:df, proto TCP (SYN), 10.0.0.201:41806->157.240.236.34:443, len 60	[1699547942124, 1
2023-11-09 23:39:01.036	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac f6:4e:ce:23:d7:f1, proto TCP (SYN), 10.0.2.54:46778->54.169.199.91:443, len 60	[1699547941036, 1
2023-11-09 23:39:01.036	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 32:7e:36:44:bf:df, proto TCP (SYN), 10.0.0.201:53400->142.251.43.195:80, len 60	[1699547941036, 1
2023-11-09 23:39:00.804	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac f6:4e:ce:23:d7:f1, proto TCP (SYN), 10.0.2.54:46776->54.169.199.91:443, len 60	[1699547940804, 1
2023-11-09 23:39:00.654	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 6c:f7:84:5f:c2:4b, proto TCP (SYN), 10.0.2.43:39504->142.251.43.228:443, len 60	[1699547940654, 1
2023-11-09 23:39:00.365	172.16.200.1	firewall,info RawLog: MikrotikGateway forward: in:Bridge_WiFi out:ether1, connection-state:new src-mac 32:7e:36:44:bf:df, proto TCP (SYN), 10.0.0.201:60476->54.77.130.51:80, len 60	[1699547940365, 1

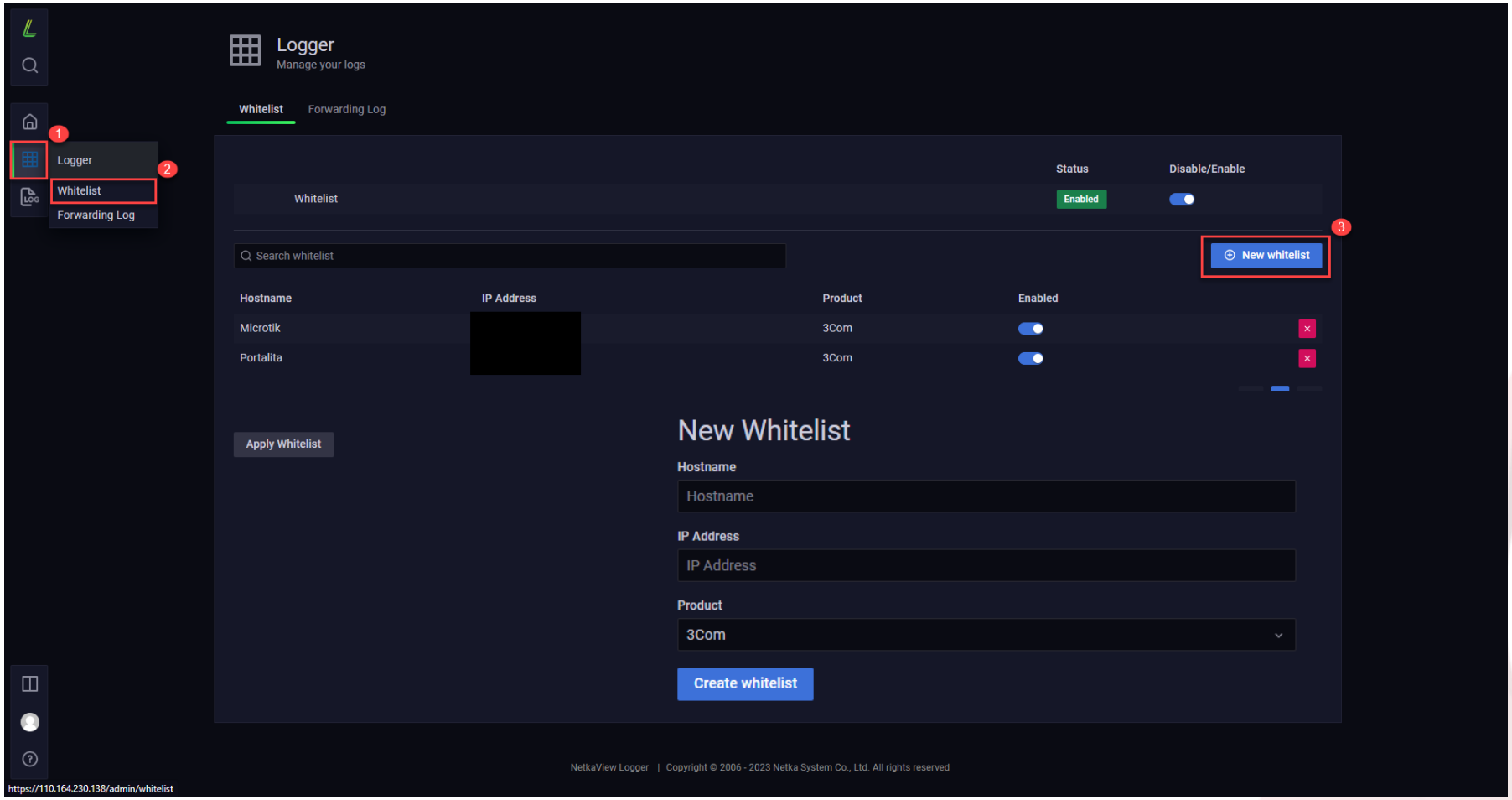
NetkaView Logger

Report PDF File



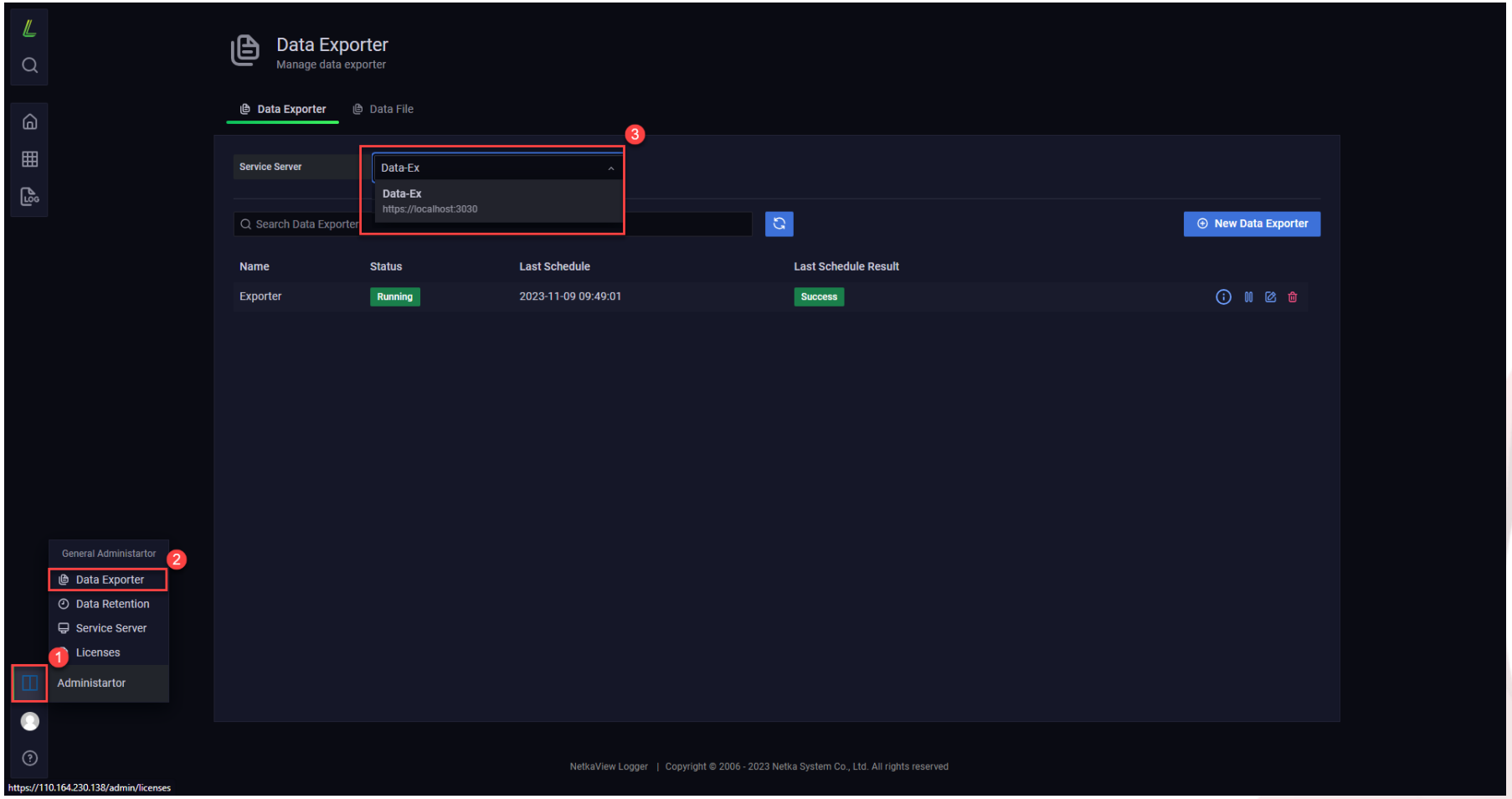
NetkaView Logger

Logger Whitelist Management



NetkaView Logger

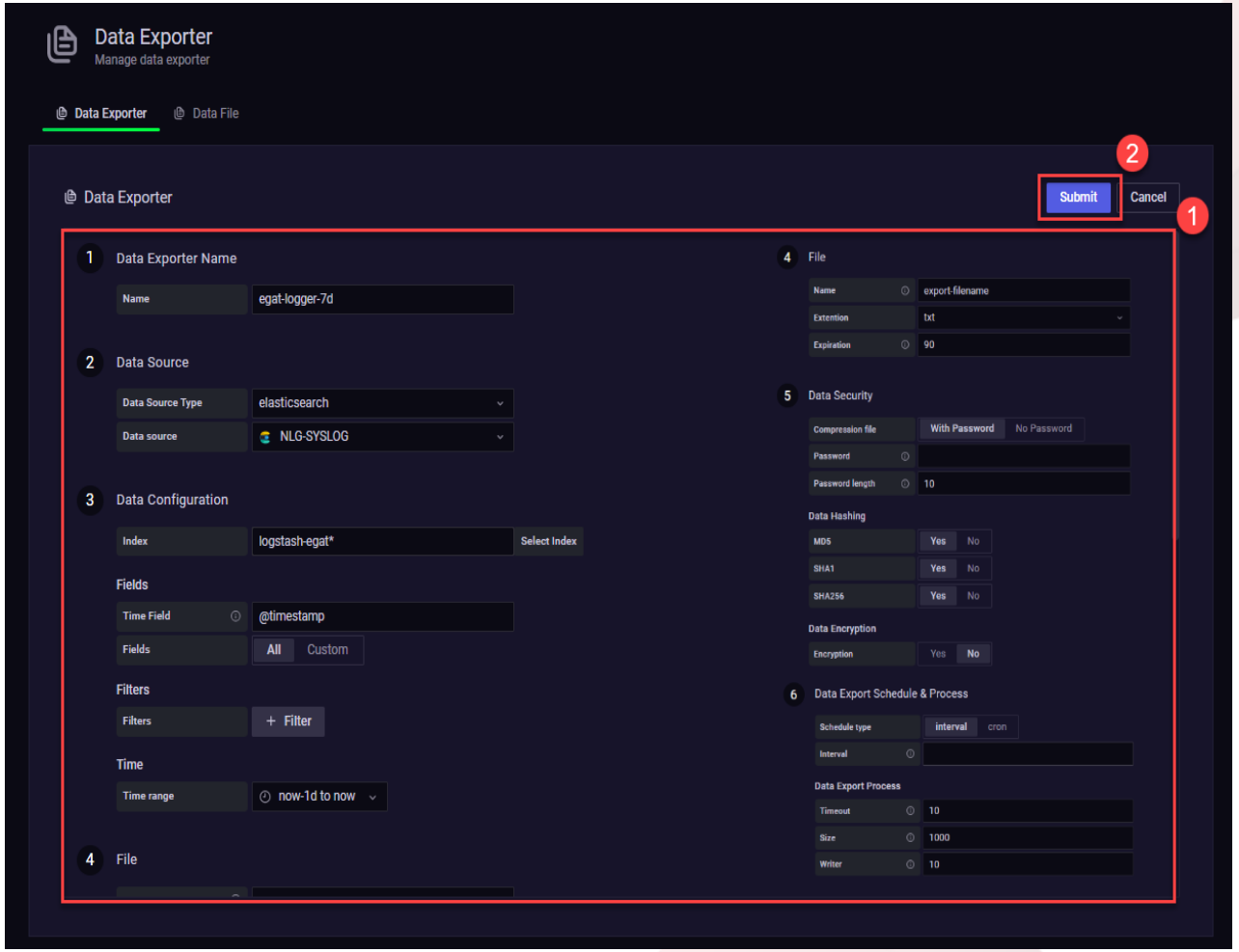
Data Exporter



NetkaView Logger

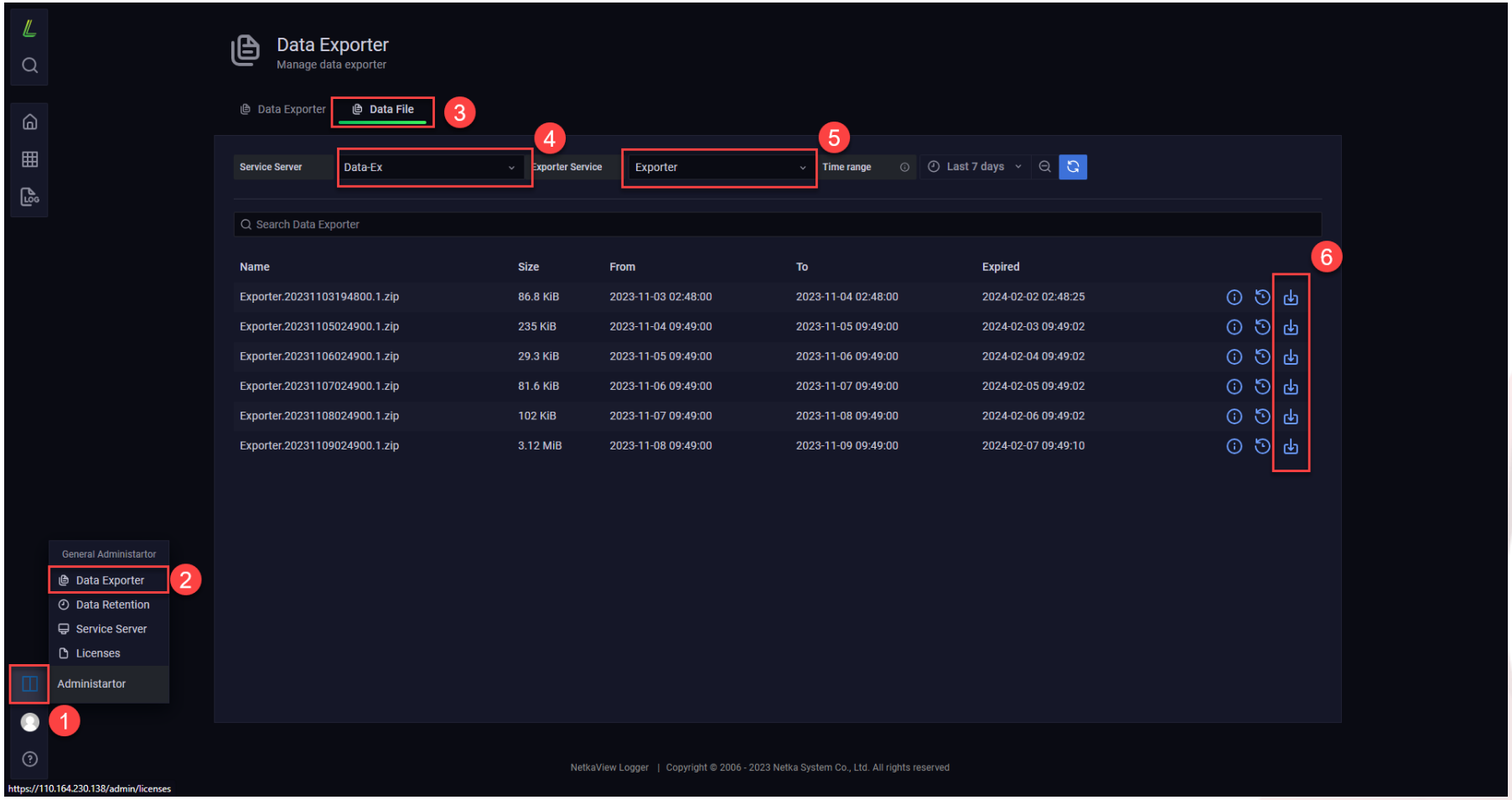
Data Exporter Schedule

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: เป็นการกำหนดช่วงเวลาที่ระเอียดมากกว่า interval โดยใช้ crontab เช่น 0 1 * * * หมายถึง ทำการ export log ตอนตี 1 ของทุกๆวัน



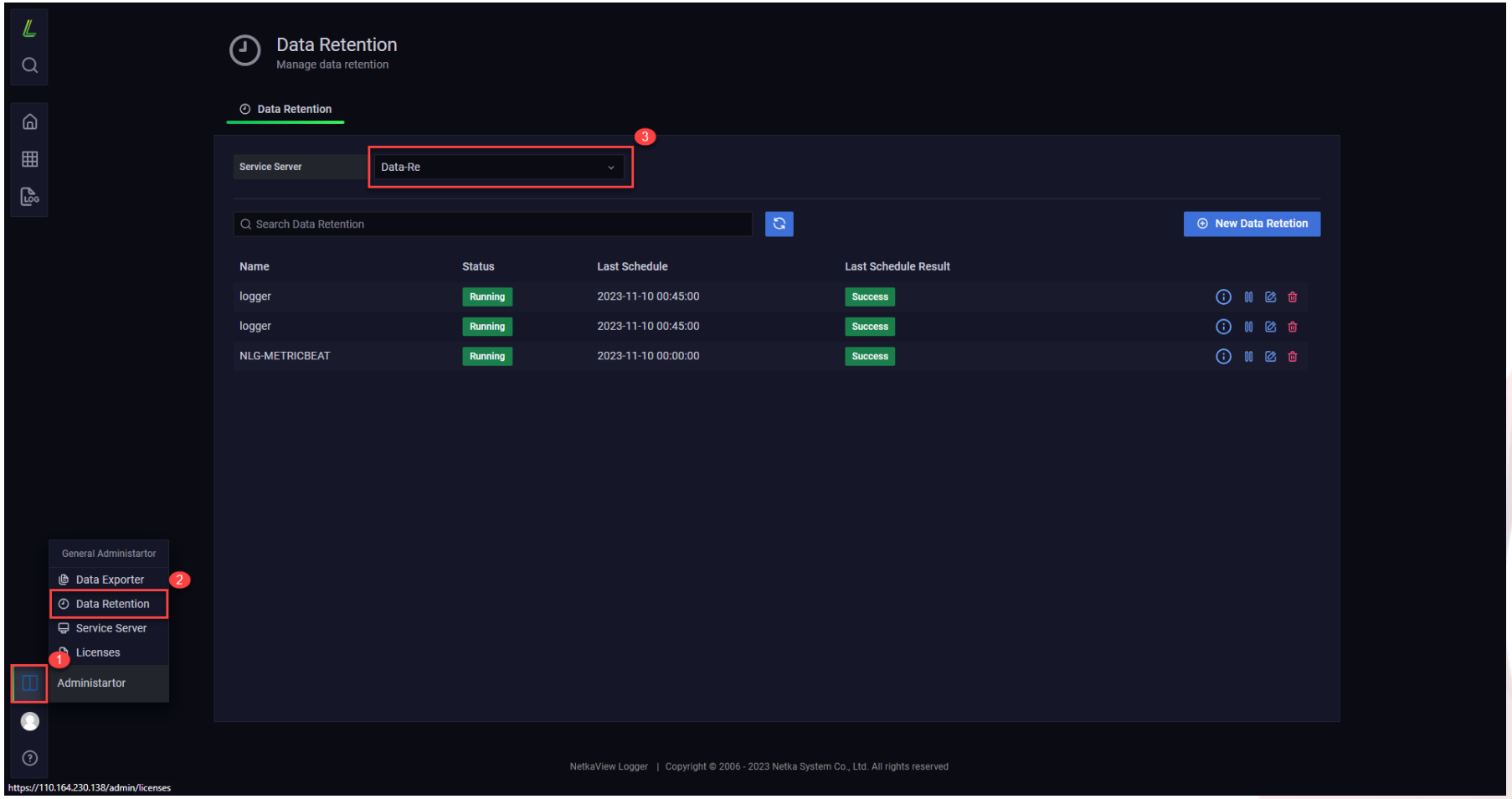
NetkaView Logger

Download Logs from Data Exporter



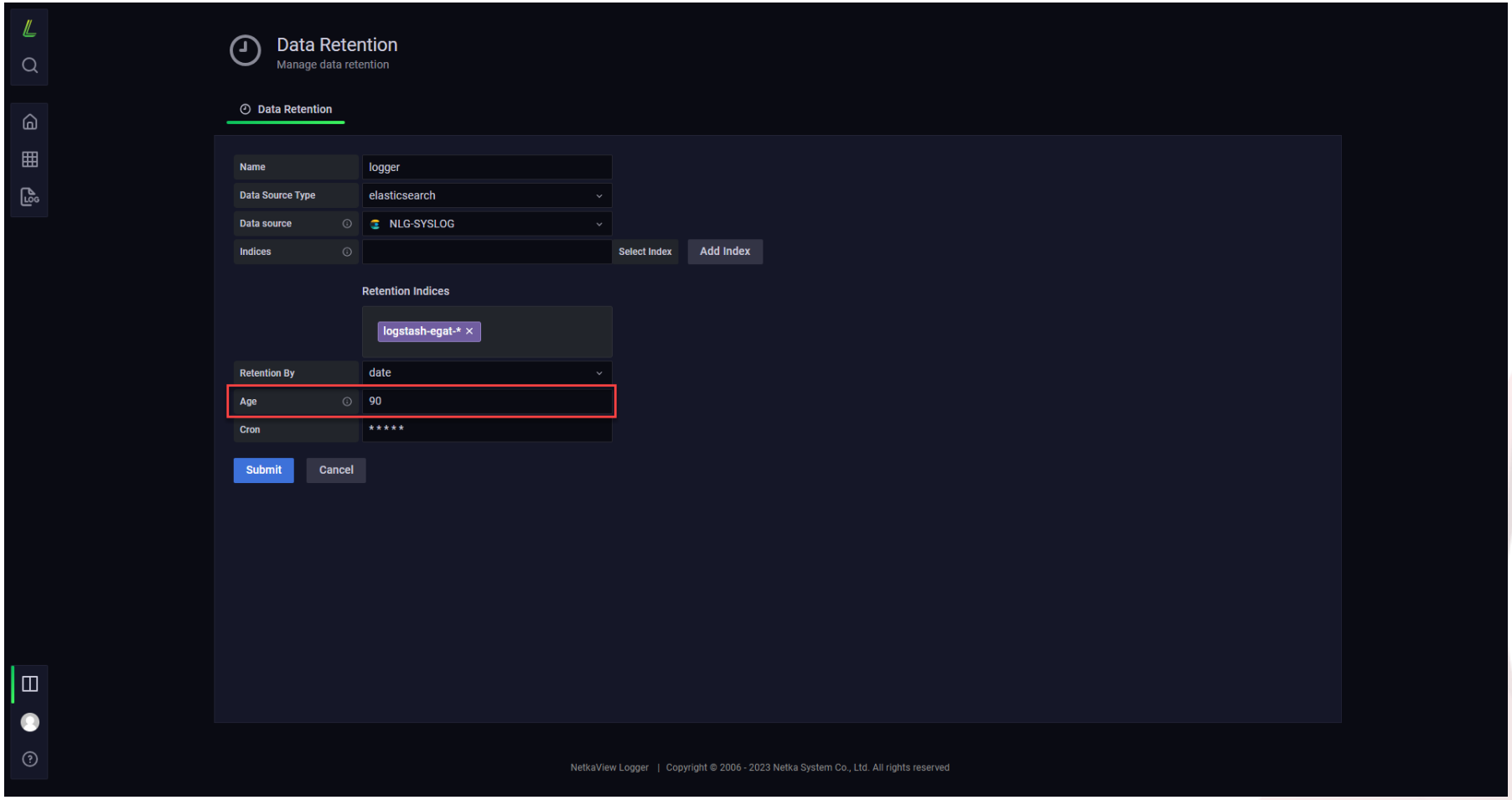
NetkaView Logger

Data Retention



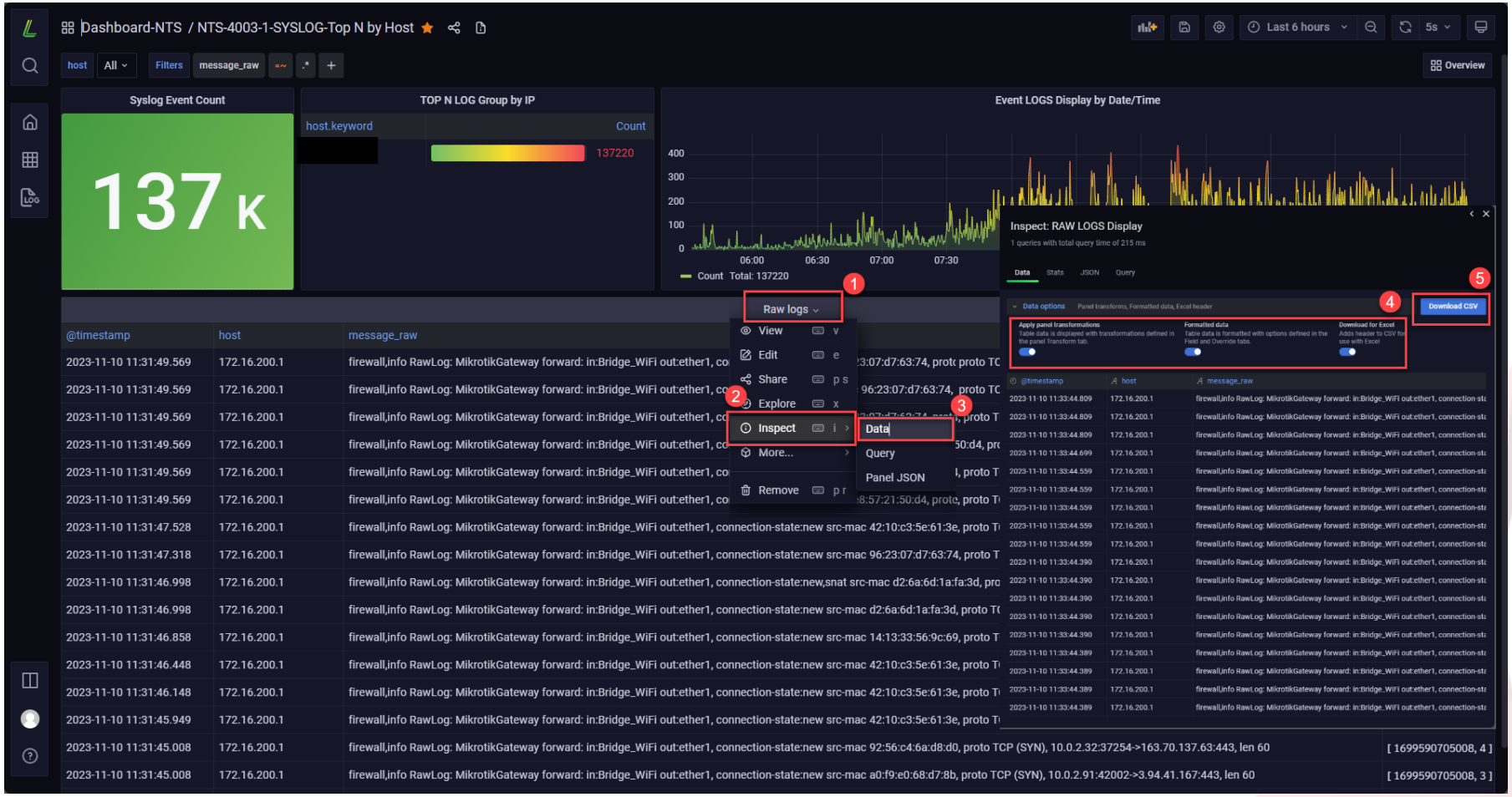
NetkaView Logger

Manage Data Retention



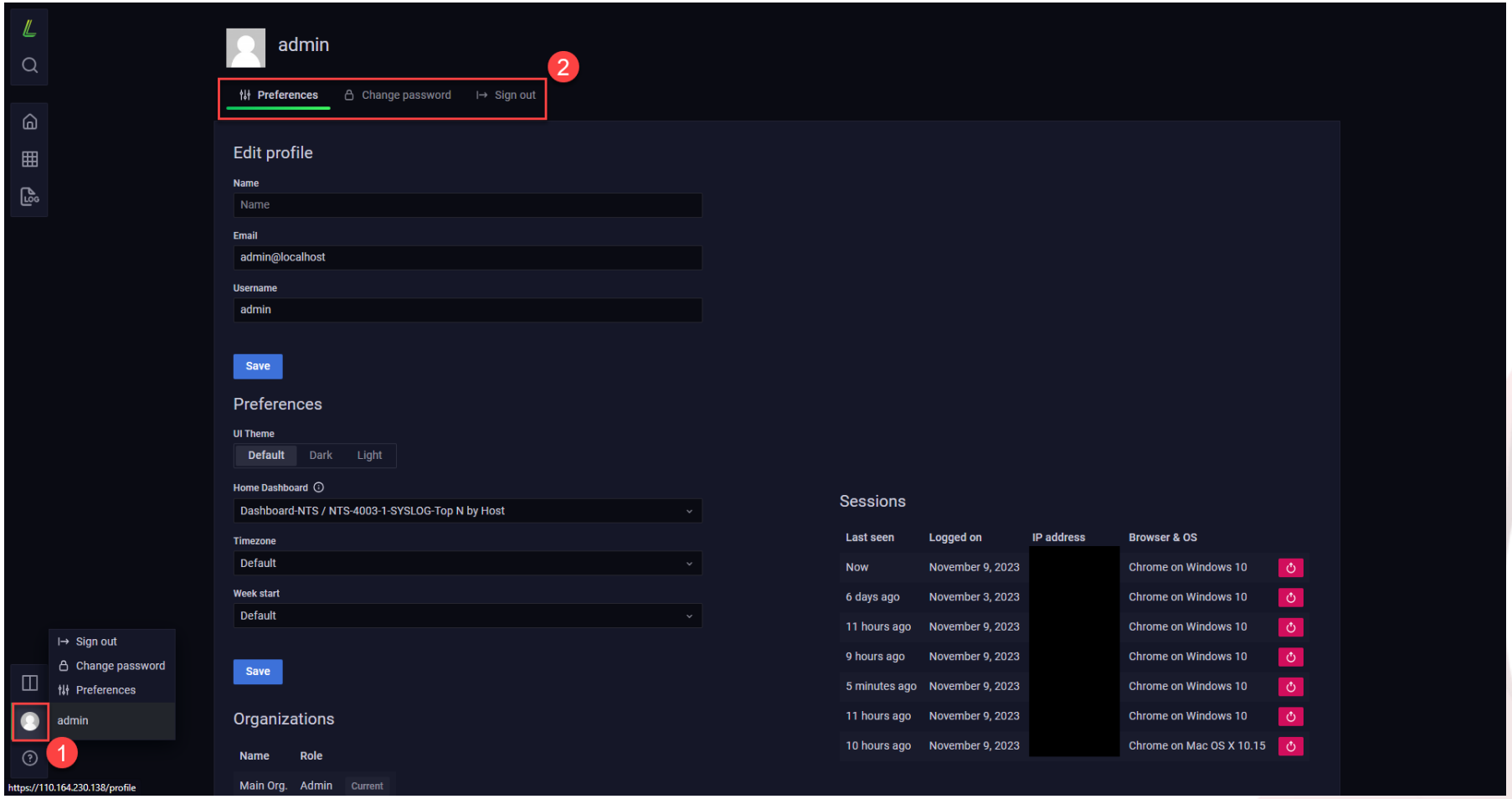
NetkaView Logger

Export Logs to CSV Files



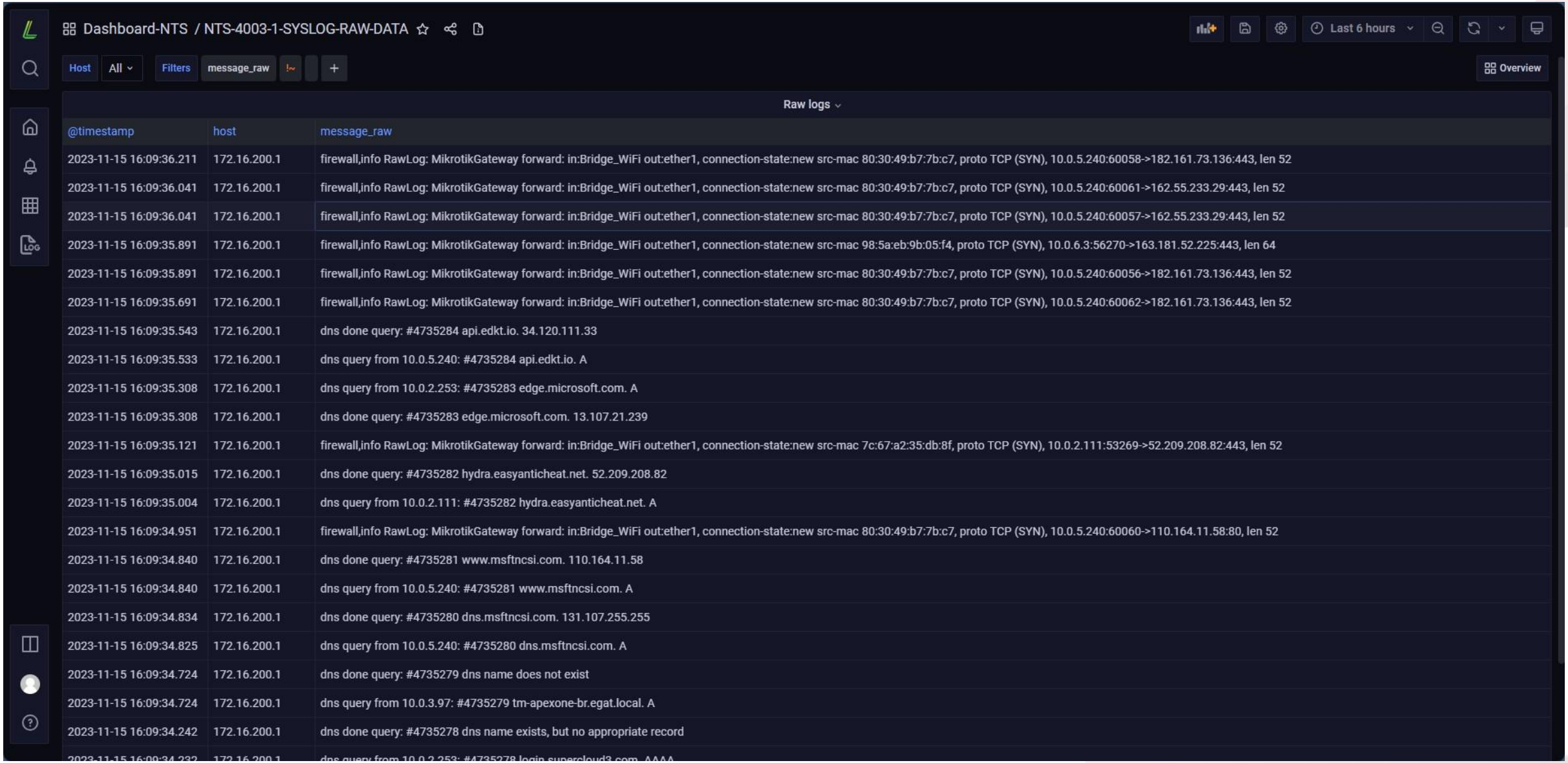
NetkaView Logger

Admin



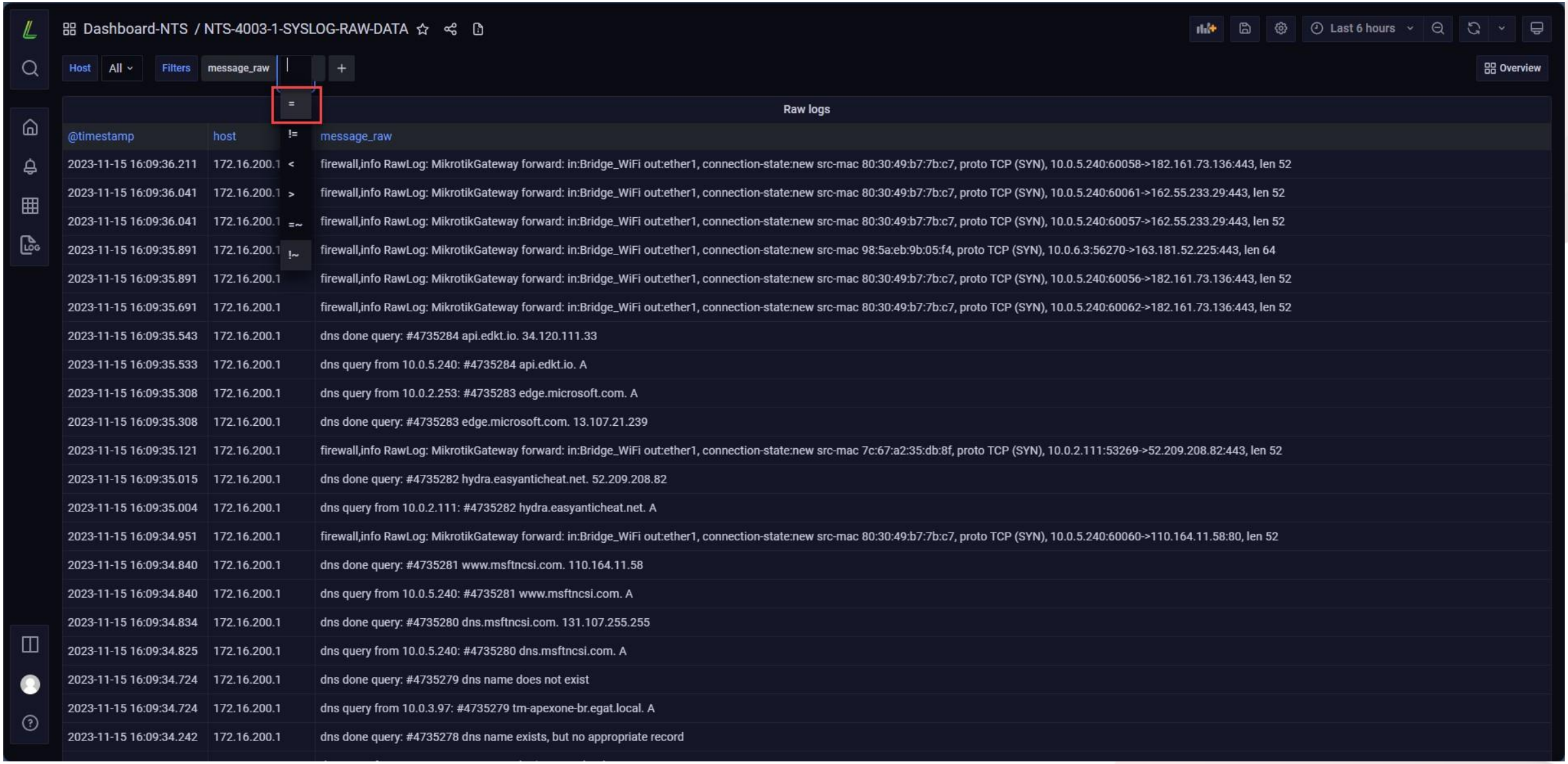
วิธีการ search

search ทุก message ที่เข้ามาในระบบ NLG เป็น default search



วิธีการ search

เปลี่ยนเงื่อนไข เป็น =



วิธีการ search

ใส่คำที่ต้องการ search