NetEvid

Keep your network activities

CENTRALIZES LOGS MANAGEMENT

Logs data storage system according to the Computer-related Crime Act.

From the Thailand Computer-related Crime Act B.E. 2550 (2007) and the Computer-related Crime Act (No. 2),B.E. 2560 (2017) on the principle of data retention of computer traffic data is a law that the person who has the relevant duties cannot deny responsibility because it is a duty and in the said act. The service user must keep the computer traffic data for at least 90 days, but in case of necessity, the authorities can order the data long-term retention up to 2 years.

NetEvid is an appliance designed to cover Logs collection to store Logs data from computer centralized aggregation, support a wide range of Logs collections from a variety of devices such as Firewall, Router, Switch, IDS, IPS, VPN, Web server, Email server, Database server, and Operating system, are displayed in the same format as well and having the ability to manage large Logs storage for a long period within the system. In addition, also can find and summarize reports within itself provided that NetEvid stores computer traffic data to records at least 90 days of Logs activities for clear audit and verified by computer traffic data storage regulations under the Computer-related Crime Act. NetEvid has also been accredited by the National Electronics and Computer Technology Center (NST 4003.1–2560).

www.netevid.com

BEST PERFORMANCE IN EVERYANGLE

High-performance work system and the flexibility

NetEvid is a device designed to store data in the NoSQL format. The advantages of NoSQL are scalable, large data support, and high flexibility, allowing NoSQL to be applied to large data and unstructured data such as storing Logs data. In addition, NetEvid optimizes Logs indexing for search and Full Text Search to improve storage and for fast searching.

NetEvid devices can support applications to meet the needs of collecting computer traffic data for customers, covering small to large organizations based on the size of the hardware devices that can support Logs from 1,500 EPS to 60,000 EPS.

In addition, for organizations that require stable performance, NetEvid devices can support the work in a way of High-Availability (HA) as well and can support scalability performance in the future.

The data is stored in the most secure storage

NetEvid is designed to provide encrypted and hashed stored data with SHA-256 for data integrity to prevent change and deletion for the integrity of the data stored and by the

Computer-related Crime Act with a Logs compression rate of 15:1, data can be stored retention more than 90 days under the requirements of the Act and can be extended the data retention up to 2 years.

NetEvid operating system is designed to highly secure, with firewall systems protected from attacks through vulnerabilities, so that stored data is highly permanent, not lost and available at all times.
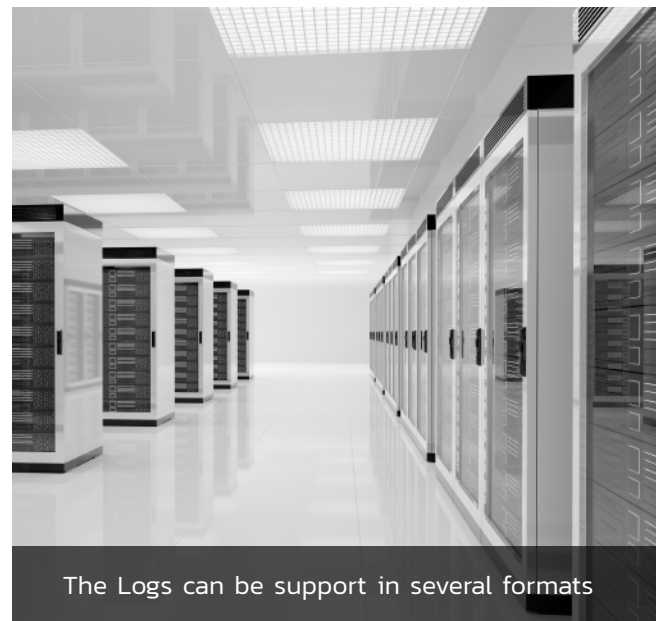
The Logs can be support in several formats

NetEvid can store Logs through the Syslogs Protocol Standard, where almost all devices send Logs mainly through this channel such as Router, Switch, Firewall System, Application, etc.

NetEvid can also store Logs from other channels in case the device is unable to send the SysLogs, only some brands of devices will send Logs via OPSEC Platform and FTP Protocol. NetEvid devices have been developed with OPSEC Agents and FTP Agents to receive Logs from that device.

The Logs can be forwarded to other devices

NetEvid can be deployed in forwarder mode to forward Logs to 3rd party devices such as forwarding to SIEM for further analysis. Alternatively, NetEvid acts as caching by storing Logs first and then selecting to send some types of Logs to SIEM for further analysis thereby reduces the Logs data to be sent to SIEM, etc.

Reports can be prepared in a variety of formats

NetEvid comes with the ability to create Logs reports from devices such as Firewall, Proxy, Active Directory, and Exchange into the report for each device such as Top N and is customizable in several formats including PDF, RTF, XML, XLS, CSV, HTML, TEXT, DOCX, and OpenOffice.

NetEvid can create Ad-hoc reports in daily, weekly, or monthly formats by filtering specific devices to be displayed in the reports and also supporting scheduling reports, and delivering completed reports can be sent to the administrator's E-mail.

Key Feature

- Centralized Logs Management to compliance requirements.

- Fully integrated and extremely fast for Logs collection.

- Logs indexing for fast Logs searching.

- Support Logs retention and searches up to 2 years.

- Highly Logs secured with SHA-256 Hashing and Archive.

- Custom reports with flexible report formats.

- On-Demand and schedule delivery time reports can be issued.

- Supports the use of HTTPS, Command-line interfaces, and SSH.

- Supports LDAP authentication.

- Data access can be controlled by assigning permissions by dividing access into administrators, data administrators, and an unlimited number of users.

- Support Logs forwarding to other devices.

- Supports recording data with external storage devices such as External Storage or DVD.

- Power searching through multiple search conditions including Wildcard expressions, Boolean expressions, and Regular expressions.

- Ability to notify via E-mail the administrator when a device malfunctions or meets preset conditions.

- Display the average of the Logs received (Average EPS) and the maximum Logs received (Peak EPS) on a daily, weekly, and monthly.

- The ability to check the status of the devices that send to the Logs to whether it is still running.

- The ability to notify the administrator via E-mail when no Logs is sent to the system and tell the last day of Logs sent to the system.

- The ability to separate the Logs collection by the organization and separate access rights.

- Logs data can be searched from devices sending Logs via IPv4 and IPv6.

- Can work as an NTP (Network Time Protocol) Server to other devices in a common network.

⚙ Product Specification

	V120	V320	V520	V720	V1200
Software Specification					
Management	HTTPS,SSH	HTTPS,SSH	HTTPS,SSH	HTTPS,SSH	HTTPS,SSH
Performance(EPS)	1,500 EPS	3,500 EPS	5,500 EPS	7,500 EPS	15,000 EPS
No. of Users	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Devices support	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Notification	Email, Syslog, Line	Email, Syslog, Line	Email, Syslog, Line	Email, Syslog, Line	Email, Syslog, Line
Log retention	90 days+	90 days+	90 days+	90 days+	90 days+
Report	Yes	Yes	Yes	Yes	Yes
Hardware Specification					
Processor	Single Processor	Dual Cores	Quad Cores	Quad Cores	Quad Cores
Memory	4 GB	8 GB	8 GB	8 GB	16 GB
Harddisk	1TB HDD, 7.2K RPM	4TB HDD, 7.2K RPM	4TB HDD, 7.2K RPM	4TB HDD, 7.2K RPM	2 x 4TB HDD, 7.2K RPM
RAID	No	Optional	Optional	Optional	0, 1
Network	10/100/1000 BaseTX	2x10/100/1000 BaseTX	2x10/100/1000 BaseTX	2x10/100/1000 BaseTX	2x10/100/1000 BaseTX
Serial Port	No	Yes	Yes	Yes	Yes
Dual Power Supply	No	No	No	No	No
Chassis from factor	211 x 116 x 28 mm.	19" 1U	19" 1U	19" 1U	19" 1U

	V3200	V3200-S	V6200
Software Specification			
Management	HTTPS,SSH	HTTPS,SSH	HTTPS,SSH
Performance (EPS)	30,000 EPS	30,000 EPS	60,000 EPS
No. of Users	Unlimited	Unlimited	Unlimited
Devices support	Unlimited	Unlimited	Unlimited
Notification	Email, Syslog, Line	Email, Syslog, Line	Email, Syslog, Line
Log retention	90 days+	90 days+	90 days+
Report	Yes	Yes	Yes
Hardware Specification			
Processor	Octa Cores	Octa Cores	Dual Processors 8 Cores
Memory	32GB	32GB	64GB
Harddisk	2 x 8TB HDD, 7.2K RPM 2 x 480GB SSD	2 x 8TB HDD, 7.2K RPM 2 x 480GB SSD	8 x 4TB HDD, 7.2K RPM 2 x 480GB M.2 SSD
Harddisk Hot Swap	Yes	Yes	Yes
RAID	0,1,5,10	0,1,5,10	0,1,5,10
Serial Port	Yes	Yes	Yes
Network	2 x 10/100/1000 BaseTX	2 x 10/100/1000BaseTX	2 x 10/100/1000BaseTX, 2 x 10GbE (up to 6 Interfaces)
Dual Power Supply	No	Yes	Yes
Chassis from factor	19" 1U	19" 1U	19" 2U

VM series	
Support	VMware-ESX, Hyper-V, Virtual Box