N-Cloud 7

DATASHEET

Next Generation IT Operation Platform

Integrate Network Management, Flow Analysis and Log Reporting

2024/07/12

As a brand-new log analysis and management platform, N-Cloud can be used in public service organizations, enterprises, multinationals, educational organizations, telecoms as valued cloud service, etc. N-Cloud is an integrated platform which enables IT administrators to store and analyze enterprise logs and manage log data with higher efficiency. With data analysis and correlation, N-Cloud helps users improve network security. The system fits users' needs and complies with the Personal Information Protection Act.

N-Cloud uses hierarchical management; users can create independent domains for each branch and department in a corporation. This way, each domain has its own log management platform and can only view the data of their own, while IT managers in headquarter can check all event logs of the corporation in a global view to ensure the network in all domains is secure.

Software

- Collects Syslog data from various devices and brands.
- Users can query system status like version, CPU and memory utilization, Syslog/Flow data received amount, etc.
- Collects Flow data with different formats, including Netflow v5/v9/v10, sFlow, Jflow, IPFIX, etc.
- Supports Chinese/English/Japanese Web interface (HTTP/HTTPS); user authority can be modified as need.
- Users can connect to the system with Console cable or through SSH and open CLI (Command Line Interface). Provide basic network settings including IP Address, Gateway, DNS, Static Route, etc. Users can perform actions such as reboot and shutdown. Our system also supports a setup page for configuration. Additionally, users can reset the password and reset the system to default.
- Supports IPv6 environment and IPv4/IPv6 dual stack environment.
- Supports SNMP V1/V2C/V3 device monitoring, and can show which switch a particular IP is on.
- Built-in treeview, N-Cloud can add each device into a categorized list as root directory and subdirectory, and it can be folded and unfolded. When there is anomaly in any device, an icon will show right after the name and the upper folders and an alert sound will be emitted to notify users.
- Able to monitor device status with SNMP, including CPU/memory utilization, interface traffic, broadcast/error information , ICMP, and so on; users can set threshold and the system will send alerts when it is exceeded.
- The CPU/memory utilization charts has drill down function; users can click the chart to see TopN reports query by Syslog or Flow, and the system will make ranking list automatically. Users can also set OID for the devices to monitor the status as need.
- Makes automatic topology for all devices in Home network, and interfaces with different traffic amount will be marked in separate color.
- Users can input multiple criteria for logical calculation (or/not); the criteria include keyword, IP, severity, etc. The number of searching criteria is not limited.
- With IP name mapping, the system will show IP and network name in “Event” and “Report”.
- With port name mapping, users can define different name for each port as need (e.g., Port 80 as Http).
- Provides user-defined threshold report of the packet size (64/128/256/512 Bytes) in units of service/department/branch, etc.With Access Control List, users can add admin accounts to IP white list.
- Provides IP geolocation information (country category), flow correlation graphs for departmental organizations or IPs or even well-known services (such as Google/Facebook/Line, etc.) and a suspicious domain/IP database for users to perform log and flow matching functions. Additionally, the system has an automatic database update mechanism.

- Receive logs through the Syslog protocol and has built-in normalization function, which can display the date, event name, severity level, IP address, user name, packet/byte transfer amount and other information in the log in different fields of the same table.
- Built-in real-time flow analysis and statistics function. According to the monitoring criteria such as traffic source, destination IP segment, host name, username, port number, protocol, network interface, traffic output device, MAC address, country, packet size distribution and other criteria to make a TOP N report or an instant flow (Packet/Byte) line graph, and the threshold value can be customized, and the alert will be triggered if the threshold value is exceeded.
- With Flow smart analysis, N-Cloud is able to detect abnormal traffic (DDoS, Hot Scan, Port Scan, Flooding, Burst Session etc.) in real time.
- Sends commands blocking particular IP/MAC addresses to network or security devices(Firewall, switch etc.) for collaboration defense (only support devices of some brands).
- Supports automatic collaboration defense; users can define own criteria for the function.
- Users can do drill down query in reports to see detailed information.
- Built-in pie charts, bar charts, and line charts; users can make various reports as need.
- Max/Avg/PCT 95 values are shown in traffic charts.
- Users can customize columns for event display and PDF files output.
- Users can make Chinese reports and output Chinese PDF files.
- Customized PDF output LOGO and layout.
- With Windows AD analyzing function, the system can do IP mapping to get username.
- Able to provide user login and logout audit log of various systems, including Linux, Windows server 2003, 2008, 2012, 2016, and so on.
- Monitors abnormal login and sends alerts.
- Able to provide various audit reports of different databases, including Oracle, MSSQL, MySQL, etc.
- Able to provide audit reports of Windows file sharing.
- Built-in dynamic Dashboard can present information such as real-time event content, alert status, and event statistics; users can define and adjust Dashboard content, grid size and screen arrangement according to needs. There are also event statistics reports, flow graphs and system status for various time periods (one hour/day/week) for users to apply.
- With Access Control List, users can add admin accounts to IP white list.
- Able to back up Syslog original raw data.
- Records users' complete historical operation records and can output them as PDF files.
- Users can get event details through Open Interface.
- Users can set up for the system to send different types of alerts or reports to the corresponding e-mail groups.

- Able to monitor CPU, fan, and hard disk status, and send automatic abnormal alerts to administrators.
- With SNMP Trap, alert will be triggered in real time when the status of hard disk is abnormal.
- With SNMP Agent, users are able to view information about the system's operational status.
- Newest self-developed compression and storage technology; it conforms to the internationally recognized cryptographic hash, FIPS 140-2, SHA2-256, SHA2-512 and AES, ensuring the data is complete and undeniable. The compression ratio is 10:1, highly increasing storage utilization.
- Always connect to N-Partner; the system can get the latest firmware automatically.
- Supports WMI (Windows Management Instrumentation) to retrieve Windows Server logs.
- Supports real-time visualization of attack dynamics in both 2D and 3D global views.
- Able to generate the Top 1,000 report for 10 million Syslog data within 48 seconds and search for a specific IP in 100 million Flow data in just 250 seconds.
- Able to receive Syslog more than 10,000 EPS (Events Per Second) and with the highest level of Flow module can receive up to 20,000 Flow Records per second.
- Supports continuously monitor the node's availability and network quality (Round Trip Time, RTT) of the monitoring node through the ICMP protocol.
- Provides a trend prediction function that can forecast short-term and long-term future trends for the CPU/Memory/Disk utilization of managed network devices and servers, as well as for the bandwidth/quality measurement values of network links. The predicted trends are displayed in visual charts with line graphs.
- Automatically associates IP addresses with their corresponding Switch/Interface information and allow users to trace and query historical mapping records.
- Provides an application that allows users to check real-time status and receive fault notifications on their mobile devices.
- Provides a two-layer TOP N report function. For each result sorted by the first layer TOP N, new statistical aggregation criteria can be set again to generate the second layer TOP N report. The statistical aggregation criteria set in the two-layer TOP N report can be different. For example, the first layer is IP traffic ranking and the second layer can be event ranking.
- Built-in Top N module that allows users to customize and query Top N statistical reports at any time. Users can select various parameters such as time intervals, event keywords, source/destination IP addresses, source/destination ports, devices, chart types, etc., to create various types of reports, including hourly, daily, weekly, monthly, quarterly, semi-annual, and annual reports.
- Built-in event module, users can search for Syslog and Flow detailed data at any time.

- Provides a database storage days prediction function.
- Supports database backup and restoration.
- Features an automatic learning capability that utilizes historical usage data from Syslog/Flow (e.g., data from the past hour or past few days) to create a baseline using advanced algorithms. This allows the system to instantly analyze and identify abnormal spikes in events or IP traffic. We can present the occurrence of these spikes with accurate timestamps in the form of trend graphs and send out alerts to users accordingly. There is no need for manual threshold configuration as our system establishes dynamic thresholds automatically based on historical patterns and usage data.
- Built-in monitoring reports, and users can customize their own monitoring conditions based on different criteria. When abnormalities occur, the system will immediately notify the administrators.
- Users can set multiple offline reports as a group.
- Users can export analysis result and reports as different formats, like PDF, XML, CSV, and so on.
- As hierarchical management, each domain runs separately and has independent reporting analysis.
- The structure is with high availability (HA), ensuring there won't be system interrupt.

Hierarchical Management

The hierarchical management of N-Cloud meets organizations' needs for decentralized management. For example, the groups can be defined as headquarter, branches, and different departments (as shown in Exhibit 1). The data of the facilities under a branch cannot be viewed by administrators in the other branches; only the headquarter administrator has the authority to view the data of each office. N-Cloud's hierarchical management provides flexible tools that meet enterprises' management needs.

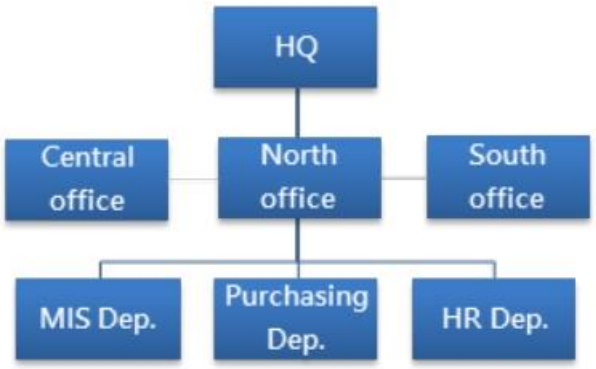


Exhibit 1

Centralized Data Management

N-Cloud collects Syslog data from network devices (Router, Switch), security devices (Firewall, IDP/IPS, Web Cache Appliance, WAF, UTM), server, database, and mainframe. N-Cloud can collect and analyze Syslog from different brands and facilities, as well as Flow data of various formats like Netflow, jFlow, sFlow, etc. Administrators can compare different data to see network security analysis, Top N ranking report, audit report, flow management, trend analysis, and abnormal attack blocking.

High Availability (HA)

With dedicated N-LB (Load Balancer), multiple N-Centers/N-Receivers can work as a redundant system (as shown in Exhibit 2), and when one is not working, the other can take over immediately. For enterprises, it's the ultimate solution, guaranteeing uninterrupted 24-hour data collection. N-Cloud accommodates unlimited Syslog and Flow source devices, without any restrictions on log or flow record quantities. It handles a minimum of 10,000 EPS for log reception, making it the ideal tool for businesses adhering to Personal Information Protection Act.

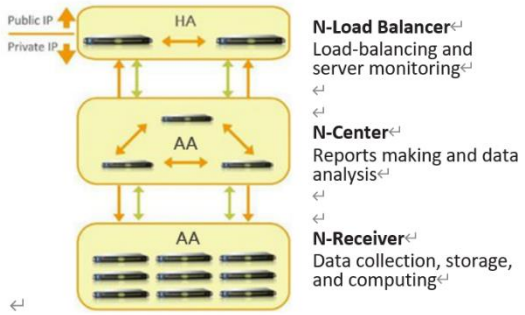


Exhibit 2

Flexible Structure

N-Cloud contains three main elements:
(1) N-LB: Does load-balancing and shows server's health status.
(2) N-Center: Processes users' query and does data cross analysis.
(3) N-Receiver: Stores and analyzes log data.
The structure provides high scalability. It can be deployed based on users' needs and adjusted accordingly for the increasing user and data in the future. It can be easily extended when received data increases.

With N-Cloud as service platform, users can create more than a thousand domains; hundreds of users can go online and query simultaneously. Take Regional Education Network Center for example; the center deploys N-Cloud as a service platform so that hundreds of middle schools can use N-Cloud, and each institute doesn't have to set up additional log service. Also, with the same service platform, it is faster, simpler to communicate when there are problems.

Specification

- Supports multiple users to use concurrently; more than 100 users can access.
- Users can set up to 1,000 different domains for branches and departments.
- Syslog: able to receive over 100,000 EPS.
- Flow: able to receive more than 100,000 EPS.
- Collects data from more than 1,000 Syslog devices.
- Users can set the saved number and time for events as need.
- Users can upgrade N-Reporter 7 to N-Cloud 7.

Multiple Query Condition for Logical Calculation and Reports

In daily operation, data query takes the most time. When there are more and more Syslog/Flow data, the ability to support flexible searching criteria and get query result fast is essential.

N-Cloud has smart query function which is combined with logical calculation and can process various kinds of query.

Columns and Parameters

- Query by Syslog or Flow
- Device
- Interface
- Time
- Event Keyword
- Username

- Source/Destination IP (CIDR or discontinues segment)
- Source/Destination Port
- Source/Destination Location
- Packet/Byte size
- Severity
- Action (Block, Permit, etc.)
- Packet/Byte number
- Policy ID
- AS Number

With logical calculation, the system can use “Or” and “Not” to get query results accord with multiple criteria. For example, if we want to query several keywords, we can put "Or" between the words; if we want to exclude certain keywords from the results, we can put "Not" in front of the words.

N-Cloud supports logical calculation of not only "keyword" but also "IP" and among different criteria. Here are some examples:

Event Keyword
P2P+Streaming: Search for all events whose name includes P2P and Streaming. P2P+Streaming!BT: Search for all events whose name includes P2P and Streaming, but exclude those with BT. [IP] 192.168.1.0/24+192.168.2.0/24 Search for all events in the two network segments.
192.168.1.0/24+ 192.168.2.0/24! 192.168.1.100-200 Search for all events in the two network segments, but exclude the events in 192.168.1.100-200.

The number of query criteria users set is unlimited; as N-Partner (Smart DB) provides N-Cloud with rapid query ability, even if there are many criteria, the searching process will not be too long.

Flow Module for Flow Analysis

Flow data (e.g. Netflow/sFlow) play an important role for traffic analysis in IT management; IT administrators learn which IP or unit uses the most network resource and which protocol (e.g. Port 80, Port 21) consumes the most bandwidth with Flow.

Flow module provides functions fitting IT administrators’ needs for Flow analysis mentioned above, such as Top N analysis and advanced drill down query, long-term Flow charts on specific targets, and Flow records of certain IPs or units.

Flow module can be used for different formats, like Netflow V5/V9, sFlow V4/V5, and JFlow; also, it can be used in the environment without Flow device but with switch mirror port. Using N-Probe, user can transfer the mirror port data and Flow information to N-Cloud.

Various Real-time Online Reports

N-Cloud's online reports show contents dynamically and contain various charts. Users can select pie chart, bar chart, and line chart as preference.

The report function also supports logical calculation (Or/ Not) so that users can use multiple criteria to make practical reports which meet users' needs, like daily reports about sever attacked events, weekly reports about traffic of employees visiting social networking sites and accessing streaming media, monthly statistics about database access, and so on.

Customized Filter Report and Anomaly Surveillance

Managers can set various filters report with different criteria to see if there are abnormal events or Flow and query with different keywords to see some particular events' timely changes. For example, monitor "Telnet/ SSH Login Fail"times to see if there are account/password guessing, monitor a server to see its connected times and traffic in midnight, monitor "Port 445" and traffic to see if there is computer worm, etc. Users can set Threshold value for filter reports, and if there is event bursting or abnormal traffic, the system will send abnormal alert email to managers.

Filter reports are with Flow module; users can make line charts about event, bps, pps, and session in the same interface to do cross reference and analysis.

Offline Report Dispatch

The system makes regular reports automatically according to the schedule; users don't have to make or export them manually. Users can set several parameters for N-Cloud to make reports, and they will be sent to the e-mail addresses users set automatically.

Report Parameters

- Severity
- Working time (daily time period)
- Working days (users can select Sunday to Saturday)
- Type (hourly, daily, weekly, semi-monthly, monthly, quarterly, semi-annual, and annual)
- Regular sending time
- Designated report recipient
- Report format (HTML, PDF, XML, CSV)

SNMP for Device Monitoring

With SNMP monitoring, users can see CPU, memory utilization and interface traffic; there are icons for users to check device status. Also, users can set threshold value as need, like set for the system to trigger alert and send notification when CPU/memory utilization is over 80% or interface traffic bursts.

The SNMP monitored devices are shown as acategorized list in treeview, and there are icons to show the status of the devices. For example, when there is anomaly in any device, a flame icon will show right after the device name, and an icon with an exclamation mark will also show after the upper folders for users to know where the anomaly is.

Built-in AI, Automatic Trend Report Based on Historical Data

N-Cloud built-in AI uses the received Syslog/Flow records to detect if there is abnormal event hit count, packet or byte, and IP, and sends alert about the event details to IT administrators for them to deal with it. Users do not have to guess or manually set threshold value; with behavior-based monitoring and analysis, users can know the anomaly in network environment, and IT operation will be easier.

N-Cloud is an event query and report making system with powerful functions, and is also an analyzer that can do actual trend analysis.

Action Module for Collaboration Defense

N-Cloud has extraordinary real-time analysis ability; users can use the results to do more advanced management. With Action module, IT administrators can precisely do further operation (usually blocking the abnormal IP) based on the severity of the security event and make the network back to normal.

Users can use N-Cloud Action Module to send IP blocking command on Web interface to the network or security devices at Internet entrance for initiate, immediate protection. (Note: Devices of some brands cannot enable this function.)

Conform to Audit Regulations

N-Cloud conforms to the cryptographic module recognized internationally, FIPS 140-2, and uses SHA-256 & AES for encryption, ensuring that the data is complete and undeniable.

https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=3002

Value-added Module (N-Probe/External Receiver)

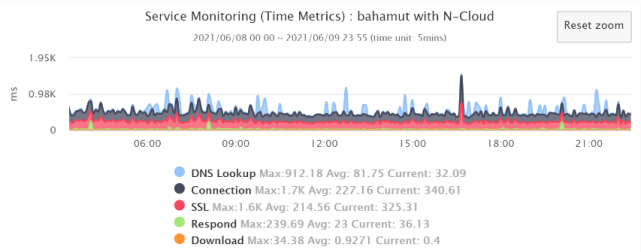
In addition to 1:1 Netflow data output and DNS analysis functions, the product of N-Partner, N-Probe, also provides the following value-added functions which users can purchase as need.

If user's network structure contains server rooms or branch offices in different geographical locations and each connects through internet/VPN, the best operation suggestion is to deploy N-Probe in all places and activate External Receiver module to collect SNMP/Flow/Syslog(including TCP and UDP) data. The data are encrypted and compressed before being forwarded to N-Reporter/N-Cloud with a compression ratio that is 5:1, greatly reducing the bandwidth load of internet/VPN and strengthening the integrity and security of the data during transmission. External Receiver can also store and forward data; when internet/VPN is disconnected , the SNMP/Flow/Syslog data will be temporarily stored and completely reforwarded to N-Reporter/N-Cloud after the connection is restored. External Receiver can be built in HA(Master/Slave) cluster for availability. Furthermore, External Receiver module includes SNMP monitoring function, which does SNMP polling to local devices to obtain IP/MAC and MAC/Port corresponding tables to assist in network management.

N-Probe also has performance monitoring (PM) module. The first function is to monitor the round trip time (RTT) of each monitored target by using ICMP ping packets; the second function is to simulate the process of people browsing web services and N-Probe will separately record the response time of several stages in the process: DNS query and response, connection establishment with web server, SSL transaction, web page response and content download; the system will make time charts with the data. To be closer to users' experience at every moment, IT

administrators can deploy N-Probe with PM module in any network location, such as office areas (OA), branch offices, and IDC leased by telecommunications carriers.

N-Probe will send the monitoring data to the intelligent IT operation platform, N-Reporter/N-Cloud, to make reports for users to view the network quality of each monitored target, achieving multi-point, multi-angle, and continuous monitoring and analysis. Besides, with the prediction function of N-Reporter/N-Cloud, it can also predict the trend in the next few hours to several months, and users can receive an alert before the delay becomes serious.



1. DNS Query and Response
2. TCP Connection
3. SSL
4. Respond
5. First Page Download

Relay Syslog and Flow

Users can define the forwarding function for Syslog and Flow data, which preserves the original source IP of the received data and forwards it to other receiving devices.

Hardware

	NP-CLD-BALANCER-EN	NP-CLD-RECEIVER-EN	NP-CLD-RECEIVER-H-EN	NP-CLD-CENTER-EN
CPU	Intel Xeon E-2334 Processor (8M Cache, 3.40GHz)	Intel Xeon E-2334 Processor (8M Cache, 3.40GHz)	Intel Xeon E-2334 Processor (8M Cache, 3.40GHz)	Intel Xeon E-2334 Processor (8M Cache, 3.40GHz)
Memory	32G DDR4 x 1	32G DDR4 x 2	32G DDR4 x 2	32G DDR4 x 2
Ethernet Controller	Dual Port GbE LAN	Dual Port GbE LAN	Dual Port GbE LAN	Dual Port GbE LAN
IPMI	Integrated IPMI 2.0 and KVM with Dedicated LAN	Integrated IPMI 2.0 and KVM with Dedicated LAN	Integrated IPMI 2.0 and KVM with Dedicated LAN	Integrated IPMI 2.0 and KVM with Dedicated LAN
I/O Port	1 VGA, 1 COM	1 VGA, 1 COM	1 VGA, 1 COM	1 VGA, 1 COM
Power Supply	350W Platinum Level	350W Platinum Level	600W Platinum Level	350W Platinum Level
SSD	500GB	500GB	500GB	500GB
HDD	N/A	12TB (4x4T with RAID 5)	4x14T with RAID 5, up to 8x14T with RAID 6	8TB (3x4T with RAID 5)
RAID	N/A	Supports RAID 0, 1, 5, 6, 10, 50, and 60	Supports RAID 0, 1, 5, 6, 10, 50, and 60	Supports RAID 0, 1, 5, 6, 10, 50, and 60
AC Power	100v-240v, 4.2-1.8A, 50-60Hz	100v-240v, 4.2-1.8A, 50-60Hz	100v-240v, 7.5A, 50-60Hz	100v-240v, 4.2-1.8A, 50-60Hz
Operating Temperature	0°C-50°C (32°F-122°F)	0°C-50°C (32°F-122°F)	0°C-50°C (32°F-122°F)	0°C-50°C (32°F-122°F)
Operating Relative Humidity	8% to 90% (Non-condensing)	8% to 90% (Non-condensing)	10% to 85% (Non-condensing)	8% to 90% (Non-condensing)
Size	1U Rackmount, 19 Inch Standard Wide RackMount Industry Server	1U Rackmount, 19 Inch Standard Wide RackMount Industry Server	2U Rackmount, 19 Inch Standard Wide RackMount Industry Server	1U Rackmount, 19 Inch Standard Wide RackMount Industry Server
Function	Built-in dedicated OS and program; able to do load balancing for connection and data receiving and be with high availability (HA)	Built-in dedicated OS and program; able to collect, query, and compute data	Built-in dedicated OS and program; able to collect, query, and compute data	Built-in dedicated OS, database, and program; provides the monitoring and user interface of N-Cloud, analyzes data, and sends alerts

VM Hardware

	NP-CLD-BALANCER-VM-EN	NP-CLD-RECEIVER-VM-EN	NP-CLD-CENTER-VM-EN	NP-CLD-E-REC-VM-EN
CPU	E-2334 (8M cache, 3.40 GHz, 8 core)	E-2334 (8M cache, 3.40 GHz, 8 core)	E-2334 (8M cache, 3.40 GHz, 8 core)	E-2334 (8M cache, 3.40 GHz, 8 core)
Memory	32GB	64GB	64GB	32GB
HDD	128GB(System)	128GB(System) 500GB/1TB/2TB(Data)	128GB(System) 500GB/1TB/2TB(Data)	128GB(System) 500GB(Data)

VM Notice

1. The VM hardware requirements mentioned above is the minimum operation requirements, please select the hardware according to actual needs.
2. Please prepare a server and install VMware ESXi 6.0 or its later versions.
3. When N-Cloud is running, in order to achieve the best performance, it will need a CPU with 8 cores or more; N-Center and N-Receiver virtual machines will need at least 64G of memory; N-LB will need at least 32G of memory.
4. When External Receiver is running, in order to achieve the best performance, memory with 32G of RAM is required.
5. Please prepare a Windows computer and install VMware vSphere Client or VMware Web Client to manage VMware Server.
6. If there is an N-Probe/External Receiver in the environment, please prepare N-Reporter/N-Cloud system to receive the incoming Flow and Syslog.
7. We provide 500G, 1T, 2T versions of N-Center VM and N-Receiver VM for users to choose. For External Receiver, there is a 500G version for users to choose.

Material

Material	Description
NP-CLD-BALANCER-VM-EN	N-Balancer VM version. Do load balancing for N-Receiver and N-Center. Include 1 year MA
NP-CLD-RECEIVER-VM-EN	N-Receiver VM version. Data receiver. Include 1 year MA
NP-CLD-CENTER-VM-EN	N-Center VM version. Provide portal, reporting and analysis result. Include 20 domains license (max up to 120 domains). Include 100 SNMP devices (max up to 1000) and 1 year MA
NP-CLD-BALANCER-EN	N-Balancer platform. Support up to 150,000 EPS. Do load balancing for N-Receiver and N-Center. Include 1 year MA
NP-CLD-RECEIVER-EN	N-Receiver platform. Data receiver. Support up to 10,000 EPS. 4T HDD*4. Include 1 year MA
NP-CLD-RECEIVER-H-EN	2U N-Receiver platform. Data receiver. Support up to 20,000 EPS. 14T HDD*4. Include 1 year MA
NP-CLD-CENTER-EN	N-Center platform. Provide portal, reporting and analysis result. Include 20 domains license (max up to 120 domains). Include 100 SNMP devices (max up to 1000) and 1 year MA
NP-CLD-E-REC-EN	External-Receiver platform. Collect and forward data. Include 1 year MA
NP-CLD-E-REC-VM-EN	External-Receiver VM version. Collect and forward data. Include 1 year MA
NP-CLD-EN-10Domains	Add 10 domains license for N-Center platform
NP-CLD-EN-100Domains	Add 100 domains license for N-Center platform
NP-EN-20SNMP	Add 20 managed SNMP devices
NP-EN-50SNMP	Add 50 managed SNMP devices
NP-EN-200SNMP	Add 200 managed SNMP devices
NP-EN-500SNMP	Add 500 managed SNMP devices
NP-EN-Ticket-G	Ticket System Module. Gold Version with 1 Year MA
NP-EN-Ticket-P	Ticket System Module. Premium Version with 1 Year MA
NP-EN-PS-T	4 Hours Training coupon
NP-EN-PS-I	One-Day Professional Service
NP-EN-PS-U	N-Reporter/N-Cloud Hardware Upgrade

Tel : +886-4-23752865 Fax : +886-4-23757458
Sales Information : sales@npartner.com
Technical Support : support@npartner.com