NETCRUNCH

КОМПЛЕКСНЫЙ МОНИТОРИНГ СЕТИ

Key Concepts

NetCrunch is designed to manage thousands of components. It allows you to manage with rules instead of individually. NetCrunch does many things automatically, so you can configure 100s nodes in just a couple of minutes. This might be a shock for you, if you are used to working with legacy tools that require individual configuration.

High Performance

NetCrunch combines the best technologies for the best results: a proprietary NoSQL database for network performance metrics history, an in-memory database for fast real-time status, and an embedded SQL database for storing alerts. It scales well on a single machine with multiple processors and several gigabytes of RAM. It can monitor over 1,000,000 performance parameters on a single server.

- Up to 1,000,000 metrics per machine
- No limit on stored data
- Raw performance data stored
- Runs on VM
- Runs in a vSphere Fault Tolerance cluster

Automatic & By Policy Management

NetCrunch allows you to detect nodes automatically and also runs an auto discovery process in the background. Once a node is discovered, NetCrunch scans its services and determines a device type or if it supports SNMP. Monitoring settings can be managed using *Monitoring Packs* which define performance metrics, triggers, and events to be monitored. Monitoring Packs can be assigned manually or automatically by rules (based on the device type or other criteria). The program also manages many views and dashboards, and automatically creates: routing maps, logical network maps and Layer 2 maps.

- IP Node Auto Discovery
- Network Services Auto Discovery
- Device Type Discovery

Built for Consistency

NetCrunch has been created for uniform data processing and visualization. In a sensor or script based tool, the monitoring logic is moved to sensors which makes it hard to update and manage. NetCrunch centralizes monitoring logic. Monitors are only responsible for delivering data and events, so all processing can be done by the server. This means that all features (like conditional alerts or performance triggers) are available for every type of event and performance data. NetCrunch supports creating both simple stateless scripts and logic based scripts.

- Uniform processing for all data sources
- Uniform visualization
- Shorter Learning Curve

Flexibility & Customization

It's impossible to list all things that can be customized in NetCruch! For instance, the console supports multiple monitors, allows docking and can automatically switch on full screen. You can create live maps with widgets showing live data or status and you can manage notifications through groups and user profiles (that can be integrated with AD). You can export data from NetCrunch, build custom scripts or get data from a web page.

- Calculated Performance Counters
- 8 Types of Performance Triggers
- Conditional Alerts
- Custom Views
- Allows Scripting & API
- Alert Escalation
- MIB Compiler
- Multiple screen & docking support

- Automated Full Screen Mode

Monitoring

NetCrunch network monitoring is built on two basic blocks: performance metrics and events. Since every monitor and sensor delivers only events and metrics, you can apply the same conditions and triggers to any of them. NetCrunch does not require any agents to be installed. NetCrunch is also extendible with scripts and data that can be pushed into NetCrunch using HTTP.

SNMP

NetCrunch uses SNMP for managing network devices (switches, printers, etc.). The program supports SNMPv3 traps and trap info packets, and includes trap forwarding. It also includes a MIB compiler and more than 3500 precompiled MIBs.

- SNMP v1, v2c, v3
- SNMP v3 Notifications and Info
- SNMP MIB Compiler
- 3500+ Precompiled MIBs

Switch and Router Monitoring

NetCrunch support various aspects of switch and router monitoring, including the status of network interfaces and bandwidth monitoring. The program automatically identifies Layer 2 connections and enables switch port mapping. Our Cisco IP SLA sensor allows you to monitor the status and parameters of IP SLA operations. NetCrunch also supports traffic monitoring and analysis and supports Cisco NBAR technology.

- Bandwidth Monitoring
- Interface Monitoring
- Routing Maps
- Port Mapping with VLAN
- Layer 2 Maps

- Traffic Monitoring
- Cisco IP SLA Sensor
- VOIP monitoring

Operating System and Server Monitoring

NetCrunch monitors the performance of Linux, Solaris, BSD and Mac OS X servers and desktops remotely via SSH. It comes with predefined monitoring settings for each system. Windows monitoring is integrated with Active Directory and doesn't require SNMP agents to be installed on servers. It allows for performance, Windows services, and Windows Event Log monitoring. You can also monitor files and folders on Windows (natively) and other systems (using FTP/s or HTTP/s). All monitors support performance metrics, process and connection monitoring.

- Windows Server Monitoring
- Linux Server Monitoring
- Mac OS X Server Monitoring
- BSD, FreeBSD, OpenBSD Server Monitoring
- Monitoring of Services, Processes, Events and Performance Metrics

Network Services & Application Monitoring

NetCrunch supports the monitoring of over 65 network services (ping, HTTP, DNS, DHCP, SSH, etc.). For each monitored service, the program checks connectivity, validates service response and measures response time.

NetCrunch can monitor an email mailbox, can alert on email content or run a round trip email sensor in order to check for mail server functionality. All sensors support secure connections. File and folder sensors support Windows (SMB) protocol, FTP (SFTP, FTPS) and HTTP/s protocols to access remote files.

- 65+ Service requests patterns
- Create custom service checks
- Apache Web sensor
- File Sensor
- Text Log sensor
- Folder sensor
- Web Page sensor
- HTTP request sensor
- Email mailbox sensors
- Email alert sensor
- Email round trip sensor

- DNS query sensors

Traffic Monitoring

NetCrunch includes a Flow Server that allows you to collect and monitor network traffic information from various flow sources using: IPFix, NetFlow (v5 & v9), JFlow, sFlow, netStream, CFlow, AppFlow, and rFlow protocols. The program analyzes traffic by various categories including: applications, protocols and domain categories. NetCrunch supports Cisco NBAR and allows you to create custom application definitions and categories.

- NetFlow v5, v9 Monitoring
- IPFix Monitoring
- JFlow, sFlow, netStream, AppFlow, rFlow Monitoring
- Cisco NBAR v2 support
- Custom Application Monitoring

Log Monitoring

NetCrunch allows you to collect and react to events from various sources. It can receive various SNMP traps (including v3 notifications) and can act as a syslog server. Additionally, NetCrunch can collect data from Windows Event log via WMI or text logs using our text file sensor.

- Syslog Server
- SNMP Trap Receiver
- Windows Event Log Monitoring
- File/Text Log Sensor

Hardware and Software Inventory

NetCrunch can collect inventory information from Windows nodes using WMI. The Inventory collects detailed data about hardware, operating system and installed software. The program also displays information on all installed patches.

- Hardware & OS Details
- Installed Software
- Installed Patches & Hotfixes
- Change Log
- Compare in time or between nodes

Custom Monitoring

NetCrunch allows you to schedule monitoring scripts or programs on the NetCrunch Server, which can then return data to the server in XML or JSON format. Alternatively, users can send data to NetCrunch using REST API. This can be done with curl or any other programing language, including popular languages like Java, C#, Javascript or Python.
See examples on Github

- Schedule Exe, JScript, VBScript on NetCrunch Server
- Send data to NetCrunch using API
- Examples on GitHub

Multi Vendor Support

NetCrunch includes primary support for Cisco, VMWare and Microsoft technologies as they are our technology partners.

The program supports various Cisco technologies including VOIP monitoring using IP SLAoperations defined on Cisco devices. The NetCrunch Flow Server supports NetFlow and Cisco NBAR technology.

NetCrunch monitors VMware ESXi v5.5/v6 including hardware health status monitoring and virtual machine monitoring. For most popular applications like MS SQL and Exchange, NetCrunch offers over 100 predefined sets of monitoring rules called Monitoring Packs.

- Cisco Monitoring
- Microsoft Monitoring
- VMWare Monitoring
- NetApp Monitoring
- HP Monitoring
- IBM Monitoring
- Oracle Monitoring
- APC, Avaya, Juniper and more...

Advanced Monitoring

NetCrunch uses advanced techniques in order to minimize false alerts, especially when monitoring remote devices over intermediate links. Monitoring dependencies control the monitoring process, so when a link is down you are not flooded with false alerts. The program also prioritizes monitoring in order to monitor intermediate links more often than remote endpoints. Monitoring packs simplify the management of monitoring parameters, so instead of changing parameters node by node, users can easily apply monitoring packs to groups of nodes. Seelist of monitoring packs

- Monitoring Dependencies
- Event Suppression
- Prioritized Monitoring
- Monitoring Packs

Alerting

Various Event Sources

NetCrunch is the primary source of various events like: status events (up/down), triggers on performance metrics or sensors and monitored statuses. The program also is also able to monitor external events by matching them with rules and triggering alerts. This allows you to trigger alerts and actions on SNMP traps, syslog messages or Windows Event log entries. NetCrunch keeps all alerts in a built-in SQL database.

- NetCrunch Status Events
- NetCrunch Sensor Events
- Performance Triggers
- Windows Event Log
- Syslog
- SNMP Traps & Notifications
- Web Message (via REST API)

Performance Triggers

One of the basic elements of network monitoring is tracking various performance metrics. Regardless of the origin of the metric, users can always use the same set of triggers to work on actual or average metric values. The average can be calculated upon a given sample number or by a given time range.

- Threshold
- Deviation Threshold
- Baseline Threshold
- State Trigger
- Flat Value
- Value Missing/Exists
- Delta
- Range

Alert Correlation

NetCrunch supports various types of correlations for alerts. Every status event generated by NetCrunch has its beginning and end, so you can easily assign an action for when the alert starts and ends. This helps you to focus only on current problems instead of checking if something is still an issue. Other events can be correlated manually, so the administrator can assign what other event ends the alert. Advanced correlation allows also you to trigger events only if multiple events have happened within a given time range, or are pending at the same time. For example, this allows you to define an alert when two redundant interfaces are down.

- Automatic Pending Alerts Correlation
- Manual Correlation of External Events
- Advanced Correlation

Conditional Alerts

The simplest condition is to trigger an alert when an alerting condition is met. But what about something that did not happen? Like a scheduled backup? Among the alerting possibilities of NetCrunch, you can define alerts for when a specific event did not happen in a certain time range, or after a specified amount of time (heartbeat not received). Other conditions allow you to suppress alert execution for some time. For example, power loss should trigger an alert after several minutes. If power is restored within a given time, no action should be executed.

- On event
- if event happen after x time
- if event happen more than x time
- Only if time range
- Only if time not in range
- If event not happen in given time range
- if event not happen after x time
- if event is pending for more x

Alerting Actions

NetCrunch allows you to execute various alerting actions like: Notifications, Logging, Control Actions and Remote Scripts. Notifications are very flexible and can be controlled by user profiles and groups. Additionally, they can be combined with node group (atlas view) membership, so it's possible to send notifications to different groups based on network node location or some other relationship. Logging actions allow you to write events to files, Windows Event log, SNMP Traps, syslog messages or triggering Web Hooks. Finally, remote actions can be executed on Windows, Linux, Mac OS X or BSD machines. There are many standard actions included like: Restarting Services, Rebooting Machines or Shutdown.

- Notifications via Email, SMS (Text Message)
- Control Actions (Restart, Run, ShutDown, etc)
- Logging (Syslog, SNMP Traps, Windows Event Log, file)
- Execute Remote Scripts & Programs
- Integration with Help Desk and Mesaging systems like Jira, ZenDesk, Slack, Twitter and many others...
- 56 Predefined Alerting Actions available

Alert Escalation & Conditional Execution

NetCrunch allows you to run actions immediately or after a certain time. This allows for escalating alert execution over time. The program also allows you to repeat the last defined action, so you may set it to keep running every day to remind you that a problem is not solved. Finally, actions can be executed when an alert is closed. Each action can be limited to run only if a triggering network node belongs to a given atlas view (these can be created by rules or manually) or within a given time range. This allows you to create flexible alerting scripts, for instance sending different notifications depending on the node location. Alerting scripts can be used for multiple alerts so you can limit actions to be executed only if an alert has a given severity.

- Run on alert start or after given time
- Run on close
- Run if severity matches
- Run only in given time range
- Run if node is member of Atlas view

Advanced Alert Processing

NetCrunch uses various technologies to avoid false alerts or protect against alert floods which might be caused by a device malfunction. When a device sends Syslog or SNMP traps to NetCrunch, the program waits for several seconds and if the same message appears several times, it won't trigger multiple alerts. Another technique (*event suppression*) is used for detecting false events caused by intermediate connection failures.

- Event Suppression
- Event Grouping

Visualization

Network Atlas

The NetCrunch Network Atlas is a central repository of all views, grouping network nodes by different categories like: nodes from the same network, nodes of a single layer 2 segment, or nodes located within the same area. It allows you to create many custom views and many of them are created automatically.

- Dynamic Views
- Dynamic View Folders
- Custom Views
- Maps, Grids and Performance Views

Dashboards

Each Atlas view has customizable dashboards. The Top Charts view aggregates information from all monitored nodes, while at the view level, dashboards show information filtered by a given node groups (like machine type or location).

- Summary Status
- Top Chart

Live Views

Most NetCrunch views are live and updated in real-time. They can be also automatically arranged. Layer 2 segment maps show port status and can also show current traffic and aggregated volume on ports. Monitoring dependencies show a diagram of dependencies that can be discovered through router and switch connections. Custom maps with widgets can show the status of network objects (nodes, interfaces, services, alerts, etc.) and current performance metrics.

- Layer 2 Segment Maps
- Routing Map
- Monitoring Dependencies
- Custom Maps
- Performance Views

Graphical Map Widgets

Graphical network maps are vital elements of network visualization. Unlike a tile based dashboard, maps show relations between elements or their location. NetCrunch maps can contain status elements for visualizing network object status and performance data widgets for showing current performance metric values.

- Node Status

- Service Status
- Interface Status
- Monitoring Pack Status
- Sensor Status
- Alert State
- 5 Performance Data Widgets

Alert & Event Views

In NetCrunch alerting, the most important view is the Pending Alerts View which help you to focus on current issues instead of a history of alerts. The history view contains all alerts processed by NetCrunch and also stores performance data for a snapshot of all performance metric based alerts. The alert summary view gives a short overview by alert category in a given time range. The history view contains many predefined views and allows you to easily create new views with a visual query builder.

- Pending Alerts
- Alert Summary by Categories
- Event History with Custom Query Views
- Performance Data Snapshots

Node Status & Details

The Node Status window quickly summarizes all information about a given network node. The Summary shows all monitored elements and their status, plus node information like system type and basic metrics (for example servers show memory, disk and network utilization). On the performance tab you can see current and last 24 hrs values of performance data. The window shows different tabs depending on the node type.

- Status Summary
- Performance Charts
- Network Services
- Interfaces
- Port Mapping on Switches
- ESX Hardware Status
- IP SLA operations
- Node Dependencies
- Node Pending Alerts & Event History

Additional Tools

NetCrunch includes additional tools for exploring node data. The SNMP Info viewer allows you to browse SNMP in an easy to understand way, with special views created for various devices. This tool also allows you to set SNMP variables. The WMI tool allows you to remotely browse WMI information. The Performance Trend Analyzer is accessible wherever performance history data is available: on node, dashboard and performance views. Finally you can customize the list of available tools in the console and let NetCrunch parameters be passed to external tools.

- SNMP Info browser
- SNMP Views Builder
- WMI Tool
- IP Tools
- Performance Trend Analyzer
- Customizable tools menu

Server

High Performance

NetCrunch Server runs on x64 Windows Server systems (*Windows 2008 R2*, *Windows 2012 R2*). It comes with its own web server and an embedded SQL database for storing monitoring events data. NetCrunch can be installed on a virtual machine, provided you assign it at least 4 processors and 4GB RAM. NetCrunch stores historical data in databases, but it processes all current data in-memory, which makes it superior in performance to SQL based solutions.

- x64 Multi Threaded Server with 4GB Ram
- In memory processing
- Built-in Web Server (with SSL support)
- Database Included
- Runs on a virtual machine
- Monitors over 600,000 performance metrics

Zero Administration Database

NetCrunch comes with a built-in SQL database for storing events generated by NetCrunch as well as events collected from SNMP Traps, syslog and Windows Event Log (WMI). For performance data, NetCrunch uses a proprietary noSQL file-based database, with no limit on the size or length of time your data is kept. Event data is accessible through the included ODBC driver, and performance data can be queried using the trend exporter (which can be also scheduled to push data to some external SQL server).

- Built-in SQL event database
- Built-in NoSQL performance data
- No limit on performance data size

Console

Remote Administration Console

The NetCrunch remote administration console can be installed on any Windows machine Windows 7 or later (32 bit or 64 bit systems). A large HD screen with 32-bit color support is required. For the best experience, we recommend multiple monitors. Additionally, 50-inch monitors will allow you to see more aspects of the monitored network. However, a Surface Pro type device with a 13-inch screen and Windows 10 will run the console smoothly.
The console always displays real-time information and requires minimal bandwidth to operate as it transmits pure data instead of HTML like many other solutions. It runs even if the network delay is more than 200ms. It can be automated to switch between defined screens automatically.

- Supports multiple monitors
- Runs over slow links
- Automatic full screen mode
- 32-bit console can be run on Vista or later
- Supports touch screen

On the go

You can browse your network status from any location using the NetCrunch Web Consolevia HTTP/S, which allows for restricting rights to particular views and operations. Console user accounts can be integrated with Active Directory. The best experience with multi screen real-time operations is available through the Remote Administration Console running on Windows desktop. NetCrunch also features a Mobile
Client designed for quick access from smartphones and tablets (iOS, Android, Windows) supporting HTML5.

- Runs in modern browser (IE10+)
- Mobile Client runs on iOS, Android, Windows Phone
- Allows access control and view restriction

GrafCrunch

The latest version of NetCrunch comes with a fork of the open source project *Grafana*. One of the top open source performance visualization projects, it greatly increases the possibilities of creating live performance dashboards and allows you to present data from various sources. The installer automatically simplifies integration of GrafCrunch with NetCrunch by creating user credentials to access data by GrafCrunch server.

- Fork of Grafana
- Open Source

Licensing

Node Based Licensing

NetCrunch is licensed per number of monitored nodes and number of concurrent remote connections to the NetCrunch server (via remote consoles). Unlike other network monitoring products, NetCrunch does not limit the number of basic parameters (network services, performance counters, and interfaces) that can be monitored on particular nodes.

- Cost effective
- Simple to manage
- No limits on data
- No sensor limits

Editions

NetCrunch comes in two editions: Premium and Premium XE. The basic difference between these two versions is scalability, so Premium is only available for monitoring up to 300 nodes. PremiumXE contains: support for a large number of nodes and more intensive processing (tuned internally to handle more work), VLAN support, Alerting Conditions, Alert Correlation, IP SLA monitoring, Event Suppression, Prioritized Monitoring, and External Events buffer.

The Corporate edition allows you to monitor unlimited number of nodes and pay per NetCrunch server deployed within an organization.

- Premium
- Premium XE
- Corporate