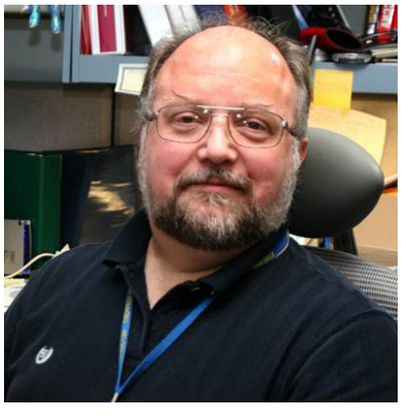
NetCrunch
real life story

Case Study
Alaska Department of Public Safety (USA)



Matt Timken
Splunk Sys Admin of the year 2007

ATLAS OVERVIEW

When the *NetCrunch Administrator Console* starts, this is the default view. I get a quick overall health view of the monitored systems and an idea what systems/services require attention.

MULTIPLATFORM MONITORING

We have quite a mixture of hardware and operating systems in our environment, from *Dell* to *HP* systems, from *Linux* to *Windows* systems, *NetApp* storage, *APC UPS*'s and *Cisco* equipment; being able to monitor all of these systems from one application has made *NetCrunch* the indispensable tool.

POLICIES

Whether using the built-in policies or rolling my own, polices allow me to rapidly change how I monitor different classes of equipment. Adding new equipment to the monitor is very easy, you just attach the new device to the appropriate policy and you're done. Reporting data and alarm processing is already done.

ALERTS/NOTIFICATIONS

I have resource owners that want to receive only messages from the devices/servers used in their daily business. I was able to define the alarms they were looking for (policies) and setup different notifications based on the alarm levels (critical, warn & info), then control how those notifications were sent to users (email or *SMS*, repeating or not). For example, when we stand-up a new *SQL* instance, I define it as a new node, assign the *SQL* policy and my resource owners start getting their required notifications.

SNMP

I like being able to roll my own views for SNMP data. I have a customized views for UPS's, *NetApp* storage appliances and *Cisco* ASA's. For example, I have included storage SNMP event for the *NetApp* storage appliances, so I will receive warnings when disk space is low on a CIFS share or iSCSI LUN. These types of warnings are available via SMS, email and visually on the *NetCrunch* map.

BACKUP/RESTORE

I have had the occasion to rebuild the *NetCrunch* database due to a server crash, restoring the database from my hourly backups saved me untold hours of work and maintained better monitoring continuity than having to restart from scratch.

NETWORK DISCOVERY AND MAPPING

Using custom maps is very handy for performing certain tasks. I have a custom view for UPS's that will show me that status of all monitored UPS's in one glance. I have similar views for Windows servers, *Cisco* ASA's and switches and *NetApp* storage appliances.

MONITORING DEPENDENCIES

We have sites that go down on occasion, that's just a fact of life in remote Alaska. Establishing the proper monitoring dependencies reduces the number of alarms generated by one of these outages to just the site router.

DAILY OPERATIONS

For daily tasks, the very first item is firing up the *NetCrunch Administration Console* and looking at the network summary, then a quick scan through the network map, followed up by going through and clearing the alarms generated overnight; some alarms require just a simple acknowledgement, others could require more hands-on attention. I use the SMS alerts to let me know that I have a critical failure in the network. I use the reports feature to give me a daily and weekly overview of the network health based on the device class; so I have summary reports for *Windows*, UPS, *Cisco* ASA and *NetApp* storage systems.

AdRem Software, Inc.
410 Park Avenue, 15th Floor, New York, NY 10022-4407, Phone: +1 (212) 319-4114, Fax: +1 (212) 832-4114
e-mail: sales@adremsoft.com