NetCrunch

Alltag eines Administrators

Wolfgang Seel
Landkreis Neunkrichen

Schneller Einstieg

Von der Installation bis zur Fertigstellung der Einrichtung von NetCrunch hatte ich keinerlei Probleme.Durch die Unterstützung des lokalen deutschen Supports war NetCrunch nach bereits kurzer Zeit einsatzbereit. Dank des hohen Automatisierungsgrades, z.B. der Netzwerkscan zu Beginn, welcher automatisch Ports und Knoten im Netzwerk ermittelt, die intuitive Bedienung und die vordefinierten Überwachungsregeln für viele gängige Geräte hatte ich ohne großen Zeitaufwand schnell die wesentlichen Geräte unter Kontrolle.

Wirtschaftlichkeit

Als städtische Institution sind wir stets angehalten Kosten einzusparen und Wirtschaftlichkeit groß zu schreiben. Aus diesem Grund haben wir zunächst einige Open-Source-Software wie Nagios ausprobiert. Aufgrund des Umfangs unserer Infrastruktur war der Bedarf an manueller Konfiguration in solchen Lösungen jedoch schlicht viel zu hoch. NetCrunch unterstützt derart viele Plattformen und Systeme, dass dieses Programm eine Vielzahl anderer Software überflüssig macht.

Das Netzwerk

Als Landkreis von Neunkirchen haben wir rund 1400 verschiedene Netzwerkdienste und knapp 600 Knoten in Betrieb, welche darüber hinaus an verschiedenen Standorten agieren. Neben klassischen auf Windows und Linux/Unix basierenden Geräten überwachen wir auch Maschinen mit VMware ESX, einen Zarafa Mailserver und die Endian Firewall mit NetCrunch.

Port-Mapping

Von großer Bedeutung ist für uns das Port-Mapping, denn es macht eine Dokumentation der physikalischen Netzwerkstruktur nicht unbedingt notwendig. Dies stellt wiederum ein großes Zeitersparnis dar und dennoch ist die Nachverfolgung von Problemen gewährleistet. Früher hatten wir für Port-Mapping ein spezielles Programm im Einsatz, welches von einem extra Administrator betreut werden musste. In NetCrunch ist diese Funktion nur eine von vielen, welche neben dem klassischen Monitoring möglich ist.

Alarmierung und Benachrichtigung

NetCrunch informiert uns stets zuverlässig über die Auslastung und Aktivität des Netzwerks und ermöglicht uns rechtzeitig Maßnahmen einzuleiten, sobald wir Engpässe feststellen. Die kritischen Teile des Netzwerks haben wir in unser Frühwarnsystem mit aufgenommen, sodass schon kleinere Absonderheiten zu einer Alarmierung führen. Wir haben für diese Situation drei Eskalationsstufen konfiguriert, wobei bei einer Minute ohne Antwort eines kritischen Knotens der zuständige Administrator via Email, SMS und direkt in NetCrunch informiert wird, nach 5 Minuten ohne Antwort die komplette EDV-Abteilung eine Alarmierung erhält und nach 30 Minuten ohne Antwort des Knotens ein OTRS Ticket versandt wird.

Kritische Funktionen unserer Infrastruktur

Sehr wichtig ist bei uns die Verfügbarkeit des DOI-Netzes zu sichern, wodurch sämtliche Behörden der Deutschen Verwaltung miteinander vernetzt sind. Mit NetCrunch kann ich einen lückenlosen Zugriff auf dieses Netz sicherstellen und somit den Mitarbeitern eine reibungslose Ausführung ihrer Arbeit ermöglichen. Ebenso wichtig für uns ist den Zugang zum Internet zu gewährleisten, da viele ihre Aufgaben und Arbeit ansonsten nicht tätigen können. Kritisch sind darüber hinaus unsere digitalen Zeiterfassungsterminals, welche von unseren Mitarbeitern nicht nur zum Check-In und Check-Out, sondern auch beim Wechseln von Räumen und Gebäuden, zur Einsicht von Urlaubstagen usw., genutzt werden. Da diese Terminals häufig beansprucht werden, haben auch Ausfälle im Bereich von 10 Minuten oft zu Verärgerung geführt. Daher prüft NetCrunch die Funktionalität dieser Terminals minütlich und informiert uns unmittelbar im Falle eines Problems.

Der Faktor „Zeit“ - Überwachungspakete

Dank der Vererbungsfunktion in NetCrunch, wodurch die Konfiguration eines Knotens direkt an andere weitergegeben werden kann, gehört eine mühsame Einzelkonfiguration der Knoten der Vergangenheit an. Schließe ich beispielsweise einen neuen SQL-Server an unser Netzwerk an, wird dieser automatisch in meine individuell erstellte Ansicht für Datenbankserver aufgenommen und es werden ohne meine Interaktion die Überwachungsregeln der anderen SQL-Server angewandt. Somit sind Änderungen im Netzwerk komfortabel und mit geringem Zeitaufwand zu bewerkstelligen.

Antizipation aufkommender Probleme

Ich habe für verschiedene für mich bedeutende und interessante Geräte die automatische Berichterstattung in NetCrunch aktiviert. So erhalte ich täglich am Morgen Informationen über das jeweilige Gerät und sehe rasch, ob es zu Problemen oder Störungen gekommen ist. Zuletzt wurde ich durch einen solchen Bericht auf eine erhöhte Fehleranzahl eines Switches aufmerksam und konnte aufgrund dessen das Gerät austauschen, ehe ein Mitarbeiter dadurch beeinträchtigt wurde.