EEN NETWORK MANAGEMENT SYSTEM VOORKOMT DOWNTIME

Netwerkmonitoring cruciaal in kritische omgevingen

Networkmonitoring levert de informatie die netwerkbeheerders nodig hebben om in real time te bepalen of een netwerk optimaal functioneert. Storingen die op korte termijn voor downtime kunnen zorgen komen naar voren, DDoS-aanvallen worden zichtbaar. *Tekst: Mels Dees*

Systemen voor network monitoring zijn onder andere software- en hardwaretools die verschillende aspecten van een netwerk kunnen volgen, zoals verkeer, het gebruik van bandbreedte, de belasting van CPU's en de uptime van alle in het netwerk verbonden devices.

Netwerkbeheerders vertrouwen op een Network Management Systeem (NMS) voor een snelle detectie van apparaat- of verbindingsfouten of problemen zoals verkeersknelpunten die de datastroom beperken.

Een NMS rapporteert over de prestaties van netwerkcomponenten in een bepaalde periode. Door een analyse van deze rapporten kunnen netwerkbeheerders voorzien wanneer de organisatie moet gaan denken aan upgrades of aan de implementatie van een nieuwe IT-infrastructuur.

Een NMS helpt organisaties daarnaast om te begrijpen hoe 'normale' prestaties eruitzien voor hun netwerken. Zo is het als er zich ongebruikelijke activiteiten voordoen (zoals een onverklaarde toename van netwerkverkeer tijdens een DDoS-aanval) eenvoudiger voor beheerders om het probleem snel te identificeren.

Het proces van netwerkbewaking wordt eenvoudiger en geautomatiseerd met behulp van software en tools voor netwerkbewaking. Deze tools zijn essentieel om netwerkknelpunten en problemen aan te pakken die van invloed zijn op de netwerkprestaties.

Grofweg biedt een NMS de netwerkbeheerders drie grote voordelen:

1 IT-downtime voorblijven

IT-downtime treedt op vanwege menselijke fouten, configuratieproblemen en andere factoren. Door een netwerkbewakingssysteem in te zetten, kunnen beheerders hun IT-infrastructuur beschermen tegen deze downtime en het optreden ervan. Bovendien geeft de monitoringsoftware-oplossing beheerders de vereiste zichtbaarheid, zodat zij op de hoogte kunnen blijven van mogelijke netwerkproblemen. Netwerkbewakingsoplossingen helpen zo om direct storingen te identificeren die de problemen met de IT-downtime kunnen veroorzaken.

2 Problemen snel identificeren en oplossen

Tijdens downtime gaan tijd en moeite verloren. Of het nu gaat om onregelmatig netwerkverkeer of een configuratiefout, de netwerkbewakingsoplossing helpt IT-teams om de problemen op te lossen door de oorzaakanalyse te vinden. Live netwerktopologie biedt de benodigde inzichten over de bron van het probleem of probleem en biedt updates over de live prestaties van netwerkapparaten. Ook helpen netwerkbewakingstools om problemen automatisch op te lossen zonder handmatige tussenkomst.

3 Cyberveiligheidsdreigingen verminderen

Een netwerkbewakingsprogramma stelt IT'ers in staat om datalekken te bestrijden door het beveiligen van de bedrijfskritische gegevens.

De basisfuncties van een NMS
Een NMS biedt in principe vier basisfuncties: Ontdek, Breng in kaart, Monitor en Alarmeer.

1 Ontdek

Netwerkbewaking begint met het detectieproces. Als je niet weet wat er op het netwerk zit en hoe het verbonden is, kun je niet monitoren of controleren. Een NMS ontdekt automatisch de apparaten op het netwerk. Het systeem beschikt daartoe over een uitgebreide bibliotheek met bewakingssjablonen, die bepaalt hoe de verschillende apparaten geconfigureerd moeten worden.
Voor effectieve netwerkmonitoring is het echter niet genoeg om te weten wat er op een netwerk is, het is ook van belang te weten hoe het allemaal met elkaar verbonden is.
Een prestatieprobleem op het ene apparaat kan immers van invloed kan zijn op het functioneren van een ander device. Wanneer een switch bijvoorbeeld uitvalt, kunnen alle apparaten die op die switch zijn aangesloten, niet via het netwerk communiceren.

Een NMS helpt organisaties om te begrijpen hoe 'normale' prestaties eruitzien voor hun netwerken

2 Breng in kaart

Netwerkbewakingssystemen genereren netwerkkaarten. Dit zijn krachtige first response tools waarmee beheerders hun netwerken kunnen visualiseren. Ze bieden een overzichtelijke en ordelijke weergave van de bedradingskast inclusief de up-to-date status van alle netwerkonderdelen.

3 Monitor

Network Monitoring Systems bieden turn-key device rollen die bepalen wat concreet gecontroleerd moet worden. Netwerkbeheerders kunnen daarbij overigens specifieke apparaatrollen wijzigen of opnieuw definiëren. De meeste netwerk monitoring tools maken het ook mogelijk secundaire hardwarecomponenten, zoals de ventilatoren en voedingen, te checken.

4 Alarmeer

Beheerders ontvangen een melding als apparaten uitvallenvia e-mail, SMS of logging.
Beheerders kunnen zelf drempelwaardes bepalen. De NMS is dan bijvoorbeeld geconfigureerd om een waarschuwing uit te sturen wanneer het CPU-gebruik op een router meer dan 80% bedraagt gedurende langer dan 20 minuten. Hierdoor kan de netwerkbeheerder proactief onderzoek verrichten en tijdig reageren voordat de router helemaal uitvalt.

Standaardprotocollen
Netwerkbewakingssystemen peilen netwerkapparaten en -servers voor prestatiegegevens met behulp van standaardprotocollen zoals SNMP, WMI en ICMP.

SNMP (Simple Network Management Protocol)
SNMP is een standaardprotocol dat gegevens verzamelt van bijna elk aangesloten apparaat, waaronder routers, switches, draadloze LAN-controllers, draadloze access points, servers, printers en meer.
SNMP werkt door "Objecten" op te vragen. Een object is iets waar een NMS informatie over verzamelt. CPU-gebruik is bijvoorbeeld een SNMP-object.
De door SNMP opgevraagde objecten worden bewaard in een beheerinformatiebasis of Management Information Base (MIB). Een MIB definieert alle informatie die wordt gegenereerd door het beheerde apparaat. De MIB voor een Cisco-router bevat bijvoorbeeld alle objecten, gedefinieerd door Cisco, die worden gebruikt om die router te controleren, zoals CPU-gebruik, geheugengebruik en interfacestatus.

WMI (Windows Management Instrumentation)
WMI is een protocol dat wordt gebruikt voor het monitoren van Windows-servers en Microsoft-applicaties. WMI is specifiek voor Windows en controleert geen netwerkapparaten of niet-Microsoft-servers.

ICMP
Netwerkapparaten, zoals routers en servers, gebruiken het Internet Control Message Protocol om informatie over IP-activiteiten te versturen en om foutmeldingen te genereren bij apparaatstoringen.

Volgens onderzoek van Cisco wordt 95 procent van de netwerkwijzigingen nog altijd handmatig uitgevoerd

Automatisering van het beheer
De afgelopen jaren hebben bedrijven enorme vooruitgang op het gebied van digitalisering geboekt. Toch riskeren bedrijven die niet actief hun processen automatiseren, kosten verlagen en de klantervaring verbeteren alsnog de boot te missen. Het belangrijkste fundament hierbij is het netwerk. Volgens onderzoek van Cisco wordt 95 procent van de netwerkwijzigingen nog altijd handmatig uitgevoerd. Dat resulteert in operationele kosten die twee tot drie keer hoger zijn dan de kosten van het netwerk zelf. Het komt er in de praktijk op neer dat bedrijven tijd, moeite en geld verspillen met oude technologieën die de tand des tijds niet hebben doorstaan.
Virtuele netwerken helpen bedrijven om hun automatiseringsniveau te verhogen. Dit maakt een snellere uitrol van nieuwe diensten mogelijk en betekent bovendien minder beheerskosten en een snellere oplossing van problemen. In de afgelopen jaren hebben veel bedrijven bovendien de manier waarop ze de prestaties van IT meten veranderd. ■