LANline

10,– €

Oktober 2017
22. September

ITP VERLAG

IT ■ Network ■ Datacenter www.lanline.de

Security in der Cloud

Hype um KI und ML für die IT-Sicherheit

Handlungsdruck durch EU-DSGVO

Mit Marktübersicht Verschlüsselung für mobile Endgeräte

Veritas NetBackup 5240 Appliance im Test
Komplettpaket für die Datensicherung

Windows Server 2016 und DNS
Sicherheit per Richtlinie steuern

Schwe… Phy…
M…

Integrated-Service-Monitoring aus Deutschland

Made in Germany

Die IT-Infrastruktur zu managen und zu betreiben gilt heute zunehmend als Mammutaufgabe. Einerseits sind Unternehmen von IT als Produktionsfaktor stark abhängig, andererseits sollen sie die bereitzustellenden Dienste zu immer günstigeren Preisen, mit möglichst kurzen Bereitstellungs- und Ausfallzeiten, unter maximal möglichen Sicherheitsbedingungen mit immer weniger Personal erbringen können.

Auch Cloud-Dienste und XaaS („Everything as a Service“) konnten bisher keine abschließende und befriedigende Lösung bringen, da Unternehmen aus verschieden Gründen immer noch eine eigene IT betreiben müssen. Die nähere Zukunft wird sich folglich eher mit einer hybriden Infrastruktur beschäftigen müssen, also einer Mischung aus eigener IT und externen Diensten.

Expertensysteme

In der gesamtheitlichen IT-Infrastrukturverwaltung treffen eine ganze Reihe vielschichtiger und mächtiger Expertensysteme aufeinander. Von Konfigurationssystemen, Netzwerk- und Kabelverwaltungssoftware („Configuration“) oder Gebäude- und Gebäudeanlagenverwaltung („Facility“) für die Infrastrukturabbildung über Messwertverarbeitung sowie Monitoring bis hin zu integrierten Service- und Prozesskonsolen ist alles zu finden. Viele Systeme und deren Pflegeprozesse sind historisch gewachsen und erfüllen ihre Aufgabe sachdienlich. Es mangelt jedoch oft an einer ausreichenden Integration der Systeme, Prozesse oder Querschnittsfunktionen. Einzelne dieser Silos erfüllen bisweilen auch funktional nicht die Erwartungen. In ihrer „IT Management Landscape“ haben die Fachleute von Aixpertsoft diese Systemlandschaft mit funktionalen Silos – meist bestehend aus einer Reihe von Einzelsystemen – übersichtlich dargestellt (Bild 1).

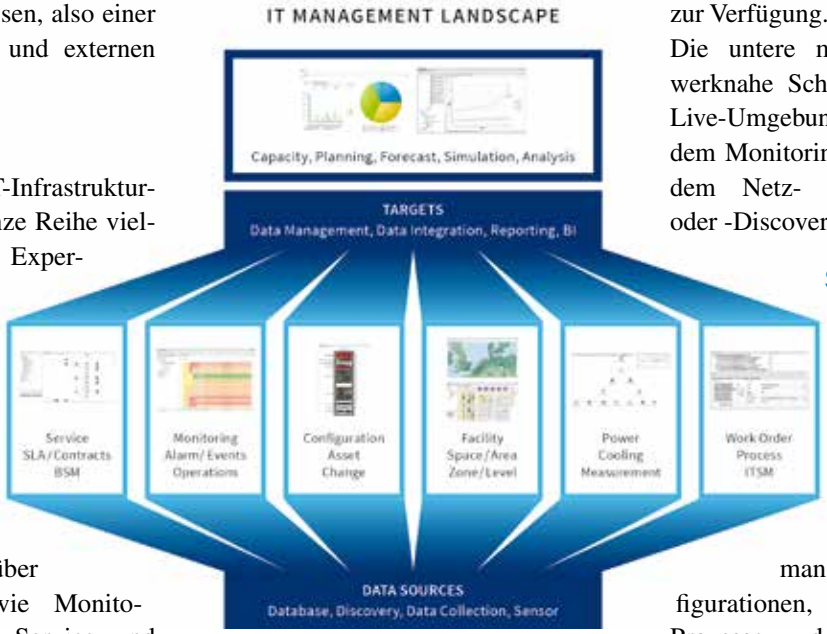

Bild 1. IT Management Landscape: Übersicht über Systemgruppen in der IT-Infrastrukturverwaltung. Bild: Aixpertsoft

Synergien sind mit der Integration von Daten und Prozessen und der Minimierung der Gesamtzahl von Einzelsystemen zu erreichen. Letztendlich gilt dies übergreifend mit der Ausrichtung der IT-Strategie an der Business-Strategie des Unternehmens. Will sich ein Unternehmen jedoch nicht mit einer umfangreichen Schnittstellen- und Integrationsstrategie befassen, empfiehlt sich die Einführung eines Data Repositories oder Umbrella-Systems, das die Aufgabe eines zentralen Datenbrokers übernimmt. Vorteile des Datenbrokers sind neben seiner Zentralität die Abbildungstiefe sowie Aktualität und Qualität der technischen Einzeldaten. Also bietet er im übertragenen Sinn ein ERP-System für die IT-Landschaft.

Das Drei-Schichten-Modell

In der Projekt- und Kundenrealität hat sich eine dreischichtige Architektur bewährt, allein wegen der Berücksichtigung bereits vorhandener Systeme und Prozesse. Die mittlere Schicht (hier CMS-Datendrehscheibe genannt) erfüllt die Aufgabe des beschriebenen Datenbrokers und stellt sowohl für die übergeordneten IT-Prozesse (häufig in ITSM-Systemen abgebildet), aber auch für kaufmännische Systeme oder Steuerungssysteme hochwertige Rohdaten zur Verfügung.

Die untere maschinennahe oder netzwerknahe Schicht liefert Daten aus der Live-Umgebung, also zum Beispiel aus dem Monitoring, der Sensorik (IoT) oder dem Netz- und System-Management oder -Discovery.

Service-Monitoring

Für eine Service-orientierte und hybride IT-Landschaft sind die in Bild 2 gezeigten Schichten in Einklang zu bringen. Zur Service-Modellierung benötigt man Architekturdaten und Konfigurationen, zur Service-Erbringung Prozesse, zudem Monitoring und Überwachung. Leider ist das Monitoring heute immer noch häufig mehr Host-orientiert als verbindungsorientiert, was zu Schwierigkeiten führt, wenn ein Unternehmen die Dienstlandschaft Ende zu Ende über höhere Layer überwachen will oder weitere Sicherheitsaspekte zu beachten sind. Die Betreiber wünschen sich durchgängi-

ge Sichten auf Services, Infrastruktur und Netzverbindungen, um so beim Troubleshooting, in der Planung und im Betrieb auf notwendige sogenannte Impact- und Root-Cause-Sichten zugreifen zu können.

Aixpertsoft und Consistec haben sich gemeinsam die Aufgabe gestellt, ihre jeweilige Kernkompetenz zu bündeln, um genau diese Lücke zu schließen. Integrated-Service-Monitoring bedeutet demnach einerseits die Service-Strukturabbildung auf Basis von konsolidierten und integrierten Infrastrukturdaten bereitzustellen, diese andererseits mit aktivem Monitoring oder Tracing in Bezug zu setzen. Der Datenbroker stellt dabei das Bindeglied zwischen aktivem Monitoring und prozessualer Verarbeitung dar und visualisiert die Zusammenhänge.

Bei der Überwachung von IT-Infrastrukturen unterscheiden Experten verschiedene Monitoring-Ansätze: Verfügbarkeit, Leistungsfähigkeit, Sicherheit und Service-Monitoring, Application Logging, Extraktion von kundenspezifischen Key-Performance-Indikatoren (KPIs), Überwachung von SLAs, Event Detection, Session-Verfolgung, Ermittlung der User Experience etc.

Wenn von Monitoring jenseits von Nagios-ähnlichen Systemen die Rede ist, dann ist meistens ein Application-Aware Network Performance Monitoring (AANPM) gemeint. Für AANPM sind im Allgemeinen keine Nutzdaten (Payload) erforderlich. Um typische Performance-Indikatoren wie Lauf- und Antwortzeiten, Protokollverteilung, Auslastung, Anzahl an Retransmissions etc. zu ermitteln, genügen die Informationen aus den Protokoll-Headern. Insofern ist der Einsatz von Flow-basierenden Monitoring-Systemen ein naheliegender Ansatz zum Performance Monitoring.

Flow-basierende Monitoring-Systeme sammeln die aus Protokoll-Headern gewonnenen Performance-Kennwerte, die von Flow-fähigen Netzwerkkomponenten wie Routern, Switches oder Firewalls stammen, und werten diese aus. Dieser Ansatz kann bei einer überwiegend homogenen Infrastruktur mit vielen Flow-fähigen Netzwerkkomponenten und bei ausschließlichem Performance-Monitoring vorteilhaft sein.

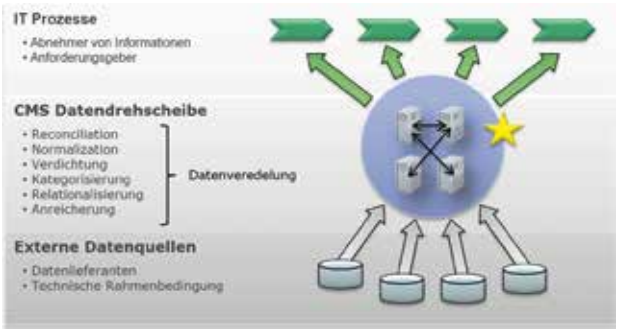

Bild 2. Drei-Schichten-Modell. Bild: Com Consult Kommunikationstechnik

Paketbasierende Monitoring-Systeme zeichnen sich dadurch aus, dass sie unabhängig von Netzwerkkomponenten und Flow-Protokollen alle übertragenen Pakete aufzeichnen können. Es ist nicht für jeden Anwendungsfall notwendig – und aus Datenschutzgründen (BDSG, EU-DSGVO, TKG) auch problematisch –, alle Pakete aufzuzeichnen. Aus diesen Gründen und zur Speicherplatzoptimierung lässt sich in der Regel bei paketbasierenden Monitoring-Systemen die Anzahl der je Paket aufzuzeichnenden Daten konfigurieren.

Noch besser ist es, wenn personenbezogene Daten oder Infrastrukturinformationen pseudonymisierbar sind. Damit kann ein Betreiber ein Optimum bezüglich des Datenschutzes unter Berücksichtigung von Analysebedürfnissen realisieren.

Ein großer Vorteil der Technik von paketbasierenden Monitoring-Systemen (Layer-7-Monitoring) ist der wesentlich breitere Einsatzbereich. Damit lassen sich beispielsweise Messwerte der Transportschicht (zum Beispiel Network Response Time) und der Verarbeitungsschicht (zum Beispiel Application Response Time) in Beziehung zueinander setzen oder kundenspezifische KPIs extrahieren sowie Service Level Agreements überwachen.

Die Datenerfassung beim Service-Monitoring sollte rein passiv erfolgen, also ohne Beeinflussung der Systeme und Dienste. Dies ermöglicht einen einfachen Rollout, und es kommt nicht zu Gewährleistungsfragen. Die vollständige Rekonstruktion der Anwendungsschicht, die nur bei garantiert verlustfreier Datenerfassung erfolgen kann, ist dabei eine notwendige Voraussetzung für korrekte Analysen und die Vermeidung von False Positives bei Alarmen. Service-Monitoring in Rechenzentren, die ihre Dienste für unterschiedliche Kunden realisieren, erfordert zudem eine Mandantenfähigkeit der Monitoring-Systeme.

Holger Nickel und
Dr.-Ing. Thomas Sinnwell/jos

Holger Nickel ist Geschäftsführer von Aixpertsoft, www.aixpertsoft.de. Dr.-Ing. Thomas Sinnwell ist CEO FuE von Consistec, www.consistec.de.

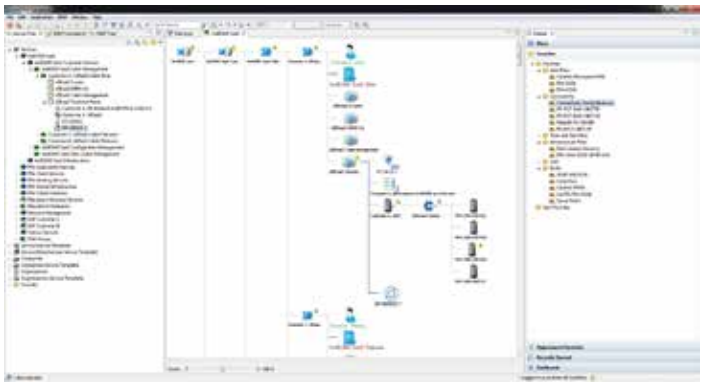

Bild 3. Service-Modell inklusive Warnung und Auswirkung. Bild: Aixpertsoft

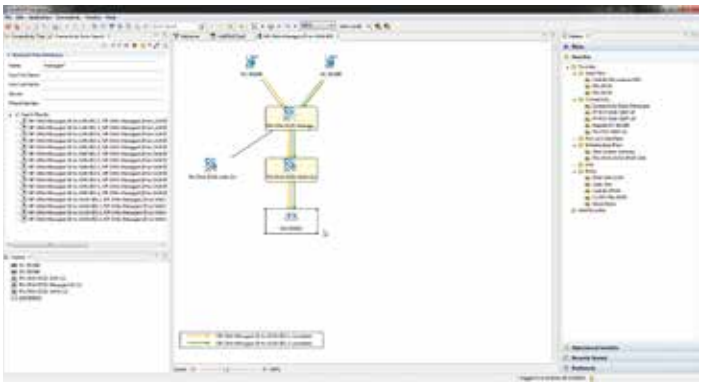

Bild 4. Überwachter Netzweg im Knoten-Kanten-Modell. Bild: Aixpersoft