

Editorial

Überblick

Netzwerk-
Provisioning

Risiken und
Heraus-
forderungen

Tool-Auswahl

Performance
Monitoring

Dokumentation




COMPUTERWEEKLY.DE



Einstieg in die Netzwerkautomatisierung

Mit Automatisierung auch komplexe Unternehmensnetzwerke in den Griff bekommen. Richtiges Provisioning, Tool-Auswahl und Dokumentation.


Home

Editorial

Überblick

Netzwerk-
ProvisioningRisiken und
Heraus-
forderungen

Tool-Auswahl

Performance
Monitoring

Dokumentation

Über die
Autoren

Netzwerkautomatisierung: Machen Sie sich die Arbeit einfacher

von *Michael Eckert*, Editorial Director bei TechTarget Deutschland

Die Unternehmensnetzwerke werden immer komplexer, und der Anteil an Virtualisierung im Data Center steigt weiter. Eine manuelle Konfiguration des Netzwerks übersteigt irgendwann die Möglichkeiten der IT-Abteilung. Der Ausweg ist eine weitgehende Automatisierung des Netzwerks.

BEI DER VIRTUALISIERUNG VON NETZWERKTECHNOLOGIEN SPIELT DIE NETZWERKAUTOMATISIERUNG EINE SCHLÜSSELROLLE.

Netzwerkautomatisierung ist eine Methodik, bei der Netzwerkgeräte per Software automatisch konfiguriert, bereitgestellt, verwaltet und getestet werden. Sie wird von Unternehmen, besonders Anbietern von Dienstleistungen, zur Verbesserung

der Effizienz und zur Reduzierung menschlicher Fehler und Betriebskosten eingesetzt.

Zu den angesprochenen Funktionen gehören einfache Netzwerkuweisungen und das Erkennen von Geräten sowie das Konfigurationsmanagement des Netzwerks und die Bereitstellung virtueller Netzwerkressourcen.

Bei der Virtualisierung von Netzwerktechnologien spielt die Netzwerkautomatisierung eine Schlüsselrolle. Damit ist eine automatisierte Bereitstellung virtueller Netzwerkmandate und Netzwerkfunktionen möglich.

Die Automatisierung wird durch eine grafische Benutzeroberfläche ermöglicht. Damit können Administratoren bestimmen, wie der Netzbetrieb durchgeführt werden soll, um ein bestimmtes Ziel zu erreichen. Dabei werden Konfigurations- und andere Managementänderungen an den Netzwerkkomponenten – unabhängig vom Hersteller – automatisch vorgenommen.

Diese E-Handbook gibt Ihnen einen Überblick zur Netzwerkautomatisierung. Dabei behandeln wir auch wichtige Punkte wie die Tool-Auswahl und die Dokumentation. ■

NETZWERKAUTOMATISIERUNG IM ÜBERBLICK

Automatisierung wird aufgrund der immer größer werdenden Komplexität der Netzwerke in Unternehmen immer dringender, um künftig agil bleiben zu können.

Von *Jessica Scarpati*

Aufgrund der zunehmenden Komplexität von Netzwerken in Unternehmen wird deren Automatisierung zur zwingenden Notwendigkeit. Denn nur so können sich Unternehmen die notwendige Agilität für neue Technologien bewahren.

Automatisierung übernimmt lästige Alltagsarbeiten und verhindert zugleich Fehler durch manuelle Eingaben. Allerdings wird der Begriff Netzwerkautomatisierung heute auf die Automatisierung aller möglichen Prozesse angewendet. Nachfolgend werden die verschiedenen Arten der Netzwerkautomatisierung erklärt.

AUTOMATISIERUNG VON LOKALEN NETZWERKEN (LAN)

In einem lokalen Netzwerk gibt es meist eine Menge unterschiedlicher Konfigurationseinstellungen und Profile, die häufig an neue Bedingungen angepasst werden müssen. Die manuelle Anpassung von [Switches](#), [Routern](#) und Tools zur Netzwerküberwachung nimmt viel Zeit in Anspruch und bietet reichlich Möglichkeiten für Fehler. Werkzeuge für Network-Konfiguration und -Management erstellen eine Datenbank mit den Geräten und Services eines Netzwerks.

Zudem spüren sie Konfigurationsfehler auf und ermöglichen Administratoren eine Fehlerbehebung ohne Ausfallzeit. Mit Tools zur Konfigurationserstellung wie der [Open-Source](#)-Software [rConfig](#) oder kostenpflichtigen Lösungen wie [Alterpoint](#) von Ignite Technologies sowie [Network Configuration Manager](#) von Solarwinds können Administratoren erforderliche Änderungen an der Konfiguration definieren. Dies erleichtert das Hinzufügen


Home

Editorial

Überblick

Netzwerk-
ProvisioningRisiken und
Heraus-
forderungen

Tool-Auswahl

Performance
Monitoring

Dokumentation

Über die
Autoren

neuer Server in das Netzwerkmodell und das Einspielen dieser Änderungen auf den entsprechenden Geräten.

Eine Automatisierung ist auch durch die im lokalen Netzwerk verwendete Hardware möglich. Beispielsweise bieten Technologien wie [Universal Port](#) von Extreme Networks und [Smartport](#) von Cisco Administratoren die Möglichkeit zur Erkennung sowie Klassifizierung der mit dem Netzwerk verbundenen Geräte. So lassen sich automatisch Skripte oder Makros für die Provisionierung von Quality of Service ([QoS](#)), [VLAN](#) und anderen Einstellungen für diesen Port verwenden. Ein IP-Telefon kann so einem bestimmten VLAN zugewiesen werden. Gleichzeitig ist auf diese Weise auch die Definition einer im Vergleich zu einer Workstation höheren Priorität für jeden einzelnen Port möglich, ohne dass der Administrator hier eingreifen muss.

AUTOMATISIERUNG VIRTUELLER UMGEBUNGEN

Hat sich ein Unternehmen für den Einsatz von Virtualisierung entschieden, sind Automatisierung und [Change Management](#) unverzichtbar. Ein wesentliches Merkmal virtueller Umgebungen sind häufige Veränderungen, die nicht unbedingt nur bestimmte Hardware betreffen. So werden ständig neue virtuelle Maschinen ([VM](#)) gestartet, wieder deaktiviert oder zwischen physischen Servern verschoben.

Eine Lösung zur Automatisierung ermöglicht diese Provisionierung anhand von Ereignissen oder Zeitplänen. Falls beispielsweise ein Controller für die Bereitstellung von Anwendungen einen Anstieg des Datenverkehrs zu einer

Webanwendung verzeichnet, kann er in der virtuellen Umgebung den Start einer zusätzlichen VM anfordern. Mit deren Unterstützung lässt sich dieses temporär hohe Datenvolumen einfacher bewältigen. Pendelt sich der Datenverkehr wieder auf einem normalen Niveau ein, kann durch Herunterfahren dieser zusätzlichen virtuellen Maschine wieder für eine optimale Auslastung des Rechenzentrums gesorgt werden. Mit der Automatisierungssoftware für virtuelle Umgebungen kann man den gesamten richtlinienbasierten Prozess der Provisionierung verwalten.

AUTOMATISIERUNG VON DATA-CENTER-NETZWERKEN

Die Möglichkeiten einer Automatisierung im Rechenzentrum gehen weit über virtuelle Umgebungen hinaus. Storage-Netzwerke, Infrastruktur für IP-Telefonie und sogar die Energieleitsysteme eines Unternehmens laufen sämtlich im Data Center zusammen. Eine Automatisierung kann hier wesentlich dazu beitragen, eine reibungslose Zusammenarbeit dieser Unternehmensnetzwerke zu gewährleisten. Zum Beispiel könnte das Energieleitsystem eines Unternehmens das Rechenzentrum anweisen, weniger Strom zu verbrauchen, das dann aktuell nicht benötigte Dienste und abgemeldete Telefone ebenso herunterfahren kann wie einzelne Switch-Ports. Dieser Vorgang erfolgt völlig automatisch und ohne Eingriff durch den Administrator.

Ebenso kann ein automatisiertes Data Center die Priorisierung von Netzwerken und Servern während fest definierter Backup-Zeiten anpassen. Auf diese Weise stehen diesen Prozessen


Home

Editorial

Überblick

Netzwerk-
ProvisioningRisiken und
Heraus-
forderungen

Tool-Auswahl

Performance
Monitoring

Dokumentation

Über die
Autoren

die erforderlichen Ressourcen für eine schnellstmögliche Erledigung ihrer Aufgaben zur Verfügung. Die heute verfügbaren Möglichkeiten für eine Automatisierung bieten zwar noch keine Selbstheilung oder ein vollkommen autonomes Rechenzentrum. Allerdings übernehmen sie bereits jetzt einen Großteil der Provisionierung von Netzwerk- und Storage-Ressourcen für die Nutzer.

NETZWERKAUTOMATISIERUNG UND DIE CLOUD

Öffentliche Cloud-Dienste sind von ihrer gesamten Struktur her bereits in hohem Maße automatisiert. So kann ein Kunde bei Bedarf zusätzliche Cloud-Ressourcen etwa von Amazon buchen, die dann vollkommen automatisch und ohne Zutun eines Amazon-Mitarbeiters zur Verfügung gestellt werden. Bei nahezu allen öffentlichen Cloud-Diensten gilt ein nutzungsbasiertes Preismodell. Dabei werden benötigte Ressourcen nur bei Bedarf angefordert und anschließend wieder freigegeben.

Mittlerweile setzen auch viele IT-Abteilungen auf ein ähnliches Modell für ihre Services und [privaten Clouds](#) mit Self-Service durch die Nutzer; auch dafür ist Automatisierung nötig. Dabei geht es nicht nur um die reine Bereitstellung von Anwendungen für die Nutzer: Ein solches Modell muss auch die Provisionierung und Abrechnung der von den Geschäftsbereichen verwendeten Netzwerk-, PC- und Storage-Ressourcen berücksichtigen. Tools

JEDE NETZWERKRESSOURCE, DIE ÜBER EINE CLI ODER EINE API GESTEUERT WIRD, KANN AUTOMATISIERT WERDEN.

für die automatische Provisionierung von Servern ermöglichen der IT-Abteilung die schnelle Bereitstellung der Ressourcen für die Nutzer. Dabei spielt es keine Rolle, ob sich diese Ressourcen vor Ort oder fernab des eigenen Standorts befinden.

ARTEN VON NETZWERKAUTOMATISIERUNG

Netzwerkautomatisierung kann in jeder Art von Netzwerk eingesetzt werden, einschließlich LANs ([Local Area Network](#)) WAN ([Wide Area Network](#)), Netzwerken von [Rechenzentren](#), Cloud-Netzwerke und drahtlose Netzwerke.

Kurz: Jede Netzwerkressource, die über eine CLI (Command Line Interface, [Kommandozeile](#)) oder eine API ([Application Programming Interface](#)) gesteuert wird, kann automatisiert werden.

Bei der skriptgesteuerten Netzwerkautomatisierung werden Skript- und [Programmiersprachen](#) zur Ausführung von Aufgaben verwendet, idealerweise solche mit präzisen Auslösern und konsistenten Verfahren. Legacy-Sprachen wie [Perl](#) und Tcl sind aufgrund ihrer Verbreitung auch in der Netzwerkautomatisierung häufig anzutreffen.

Da Netzwerke jedoch immer komplexer werden, haben neuere Open-Source-Programmiersprachen wie [Python](#) und [Ruby](#) wegen ihrer Benutzerfreundlichkeit und Flexibilität an Popularität gewonnen.

Home

Editorial

Überblick

Netzwerk-
Provisioning

Risiken und
Heraus-
forderungen

Tool-Auswahl

Performance
Monitoring

Dokumentation

Über die
Autoren

Die softwarebasierte Netzwerkautomatisierung, oft als intelligente Netzwerkautomatisierung bezeichnet, wird über ein Verwaltungsportal koordiniert. Dies eliminiert die Notwendigkeit, Skriptbefehle von Hand einzugeben. Solche Plattformen bieten in der Regel Vorlagen für die Erstellung und Ausführung von Aktionen auf der Grundlage von Richtlinien in einfacher Sprache.

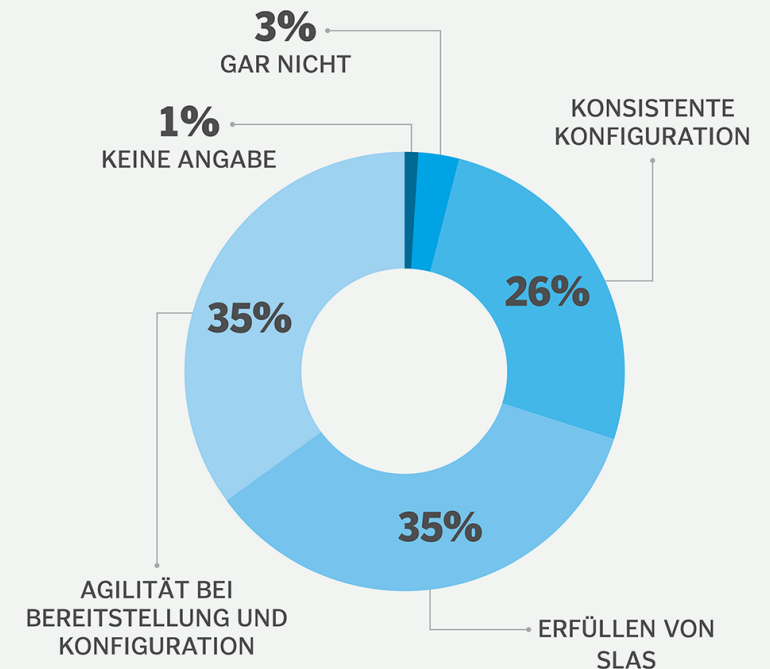
VORTEILE DER NETZWERKAUTOMATISIERUNG

Die Netzwerkautomatisierung hat drei Hauptvorteile.

- **Verbesserte Effizienz.** Durch die Automatisierung von Funktionen auf Netzwerkgeräten müssen Menschen keine zeitaufwendigen Aufgaben mehr ausführen.
- **Reduktion von menschlichen Fehlern.** Bei manuellen Eingaben unterlaufen Menschen leicht Fehler. Wenn die Stabilität eines Unternehmens- oder Service-Provider-Netzwerks auf dem Spiel steht, können die Folgen einer fehlerhaften Berechnung oder Eingabe erheblich sein. Wird hingegen die Aufgabe automatisiert, heißt das, dass sie nur einmal sorgfältig und korrekt eingegeben werden muss.
- **Geringere Betriebskosten.** Dieser Vorteil ergibt sich aus den beiden vorangegangenen Punkten. Durch den Wegfall bestimmter manueller Aufgaben im Zusammenhang mit der Bereitstellung von Netzwerkgeräten und der Netzwerkverwaltung können Unternehmen schneller und flexibler arbeiten. Beispielsweise kann die automatisierte Bereitstellung einem Netzwerktechniker die Fahrt zu einer neuen Niederlassung ersparen, um die Netzwerkverbindung herzustellen – und damit können die dortigen Mitarbeiter schneller an die Arbeit gehen.

Die Vorteile der Netzwerkautomatisierung

Wie profitieren Unternehmen von der Netzwerkautomatisierung?



QUELLE: "TRENDS IN DATA CENTER NETWORKING," ENTERPRISE STRATEGY GROUP, FEBRUAR 2016; N=306
©2016 TECHTARGET. ALLE RECHTE VORBEHALTEN.

[Home](#)

[Editorial](#)

[Überblick](#)

[Netzwerk-
Provisioning](#)

[Risiken und
Heraus-
forderungen](#)

[Tool-Auswahl](#)

[Performance
Monitoring](#)

[Dokumentation](#)

[Über die
Autoren](#)

WERKZEUGE ZUR NETZWERKAUTOMATISIERUNG

Es gibt mehrere Arten von Schnittstellen, Plattformen und Protokollen, die zur Ausführung von skript- oder software-basierter Netzwerkautomatisierung verwendet werden.

Die CLI ist das traditionellste Mittel zur Bereitstellung von Netzwerkautomatisierung. Es ist frei verfügbar und in hohem Maße anpassbar, erfordert aber Kenntnisse der CLI-Syntax.

Neben den bereits genannten Lösungen bietet ein Vielzahl von Open-Source-Tools – darunter [Ansible](#), Chef und [Puppet](#) – einen Rahmen für die Netzwerkautomatisierung.

Diese Tools verfügen in der Regel über eine Bibliothek mit allgemeinen Befehlen oder Arbeitsabläufen, die sich leicht wiederholen lassen.

Es sind auch kommerzielle Werkzeuge zur Netzwerkautomatisierung erhältlich. Die meisten Anbieter von Netzwerkinfrastrukturen haben softwarebasierte Plattformen entwickelt, die über eine spezialisierte API Automatisierungsfunktionen für ihre eigenen Produkte bereitstellen.

ZUKUNFT DER NETZWERKAUTOMATISIERUNG

Die Automatisierung ist eine der wichtigsten Methoden für die Entwicklung des [Intent-based Networking](#) (IBN), bei dem Software zur Abbildung der Ressourcen genutzt wird, um die Anforderungen der Unternehmen an ihr Netzwerk zu erfüllen. IBN wird auch künstliche Intelligenz und maschinelle Lernwerkzeuge einsetzen, um die Netzwerkabsicht weiter zu automatisieren. ■




Home

Editorial

Überblick

Netzwerk-
ProvisioningRisiken und
Heraus-
forderungen

Tool-Auswahl

Performance
Monitoring

Dokumentation

Über die
Autoren

Die Rolle von Automation beim Netzwerk-Provisioning

Automation in der IT kann Geld und Zeit sparen, ihre Einführung kann aber auch zu Problemen führen. Die IT-Abteilung muss die Prozesse deswegen sehr genau kennen. Von [Amy Larsen DeCarlo](#)

Glauben Sie ruhig dem Hype: Automation wird wesentliche Änderungen in der IT bewirken. Die IT muss Software so nutzbar machen, dass sich die Prozesse ständig an den Endkunden anpassen. Das ist nur ein logischer Schritt in einer sich schnell entwickelnden Technologie.

Die Automation in der IT wird durch Software ermöglicht. Sie führt sich wiederholende sowie vorhersehbare Aufgaben auf eine standardisierte Weise durch und befolgt dabei vorher festgelegte Richtlinien.

IT-Automation wird die Bereitstellung von Netzwerkressourcen verbessern, weil dadurch keine unnötigen Kosten entstehen und der Risikofaktor Mensch bei redundanten Aufgaben keine Rolle mehr spielt.

Die Automation in der IT schreitet bei den Management-Tools für Infrastruktur und Services sehr schnell voran. Es gibt aber Komplikationen, und einige Bereiche sind noch verbesserungswürdig.

PROZESSE IM GRIFF – DER SCHLÜSSEL ZUM ERFOLG

IT-Abteilungen kennen die Prozesse und die entsprechenden Abhängigkeiten oft nicht gut genug, um IT-Automation effizient implementieren zu können. Das gilt vor allen Dingen dann, wenn sich Unternehmen in einem größeren Umstellungsprozess befinden. Damit sind zum Beispiel Umstrukturierungen gemeint, die Änderungen bei Prozessen verlangen, die aber wiederum nicht gut definiert sind.

IT-Automation kann auch das Maß an Kontrolle reduzieren, die Experten über Unteraufgaben und übergreifende Prozesse haben. Das ist unter Umständen ein Problem, sollte eine Firma

bei der IT einschneidende Umstellungen vornehmen, bei der sich sowohl Technologie als auch Personal verändern.

Eine Integration mit existierenden Tools kann ebenfalls zu Schwierigkeiten führen. Das ist ein häufiges Problem beim Management der IT-Infrastruktur.

**AUTOMATION WIRD
WESENTLICHE ÄNDERUNGEN
IN DER IT BEWIRKEN.**



Oftmals haben die IT-Abteilungen nicht das Fachwissen im eigenen Haus, das nötig ist, um die Integration [erfolgreich durchführen](#) zu können. Das vergeudet Zeit und führt zu zusätzlichen Kosten.

INTEGRATION VON RESSOURCEN UND UNTERNEHMENSKULTUR BEIM BEREITSTELLEN VON NETZWERKRESSOURCEN

Eines der größten Probleme bei der IT-Automation ist die Unternehmenskultur und die Belegschaft. Muss die IT-Abteilung seltener manuell eingreifen, gibt es weniger Interaktion mit den Endanwendern. In Unternehmen, in denen Kontakte sehr gut gepflegt werden, kann das zu weniger Zufriedenheit beim Endanwender führen. Produziert die IT-Automation allerdings bessere Resultate, erhöht sich die Zufriedenheit sehr wahrscheinlich.

Sollten sich das Provisioning von Ressourcen und andere Aufgaben automatisieren lassen, gibt es in der IT-Abteilung natürlich die Befürchtung, dass wesentlich weniger Personal gebraucht wird. Einige Schätzungen besagen, dass sich bis zu

80 Prozent aller IT-Prozesse automatisieren lassen. Deswegen schwebt über einem Großteil der IT-Beschäftigten das Damoklesschwert der Kündigung.

BEI DER AUTOMATISIERUNG GIBT ES IN DER IT-ABTEILUNG NATÜRLICH DIE BEFÜRCHTUNG, DASS WENIGER PERSONAL GEBRAUCHT WIRD.

Um das zu vermeiden, muss die IT-Abteilung die Pläne des Unternehmens in Sachen Automation kennen und auch auf dem Radar haben, was andere Firmen tun. Die IT-Belegschaft muss ihr Wissen auf dem aktuellen Stand halten und sich notfalls auf andere Bereiche konzentrieren. Dazu gehört zum Beispiel Cybersecurity, weil hier die Nachfrage zurzeit relativ hoch ist. ■

Home

Editorial

Überblick

Netzwerk-
Provisioning

Risiken und
Heraus-
forderungen

Tool-Auswahl

Performance
Monitoring

Dokumentation

Über die
Autoren

Risiken und Aufgaben bewältigen

Viele Netzwerktechniker sind vorsichtig, was Netzwerkautomation und die damit verbundenen Herausforderungen betrifft. Dennoch führt an der IT-Automatisierung kein Weg mehr vorbei. Von [Terry Slattery](#)

Viele Netzwerktechniker und Netzwerkmanager zögern, das Thema Netzwerkautomatisierung anzupacken. Jeder, der schon einmal ein Netzwerk eine gewisse Zeit betrieben hat, dürfte einen größeren Netzwerkausfall miterlebt haben.

Größere Ausfälle sind stressig und unangenehm. Daher vermeiden IT-Teams alles, was dazu führen könnte. Wenn schon einfache Änderungen einen größeren Ausfall verursachen können, stellt sich die berechtigte Frage, warum jemand ernsthaft an den Einsatz von Automatisierung denkt, die eine schlechte Konfiguration sehr schnell über das gesamte Netzwerk verbreiten kann.

Wenn Automatisierung der Grund für ein nicht funktionierendes Netzwerk ist, werden die Teams kaum Automation als Lösung in Erwägung ziehen. Stattdessen ist das Tool der Wahl, um Fehler zu korrigieren, üblicherweise die Kommandozeile, mit der Teams ein Gerät nach dem anderen konfigurieren.

Wenn eine IT-Abteilung 100 Geräte updatet und dabei eine Minute pro Konfiguration braucht, ziehen sich die Änderungen über anderthalb Stunden hin. Multiplizieren Sie diese Zeit mit der

Anzahl der Minuten, die der Vorgang tatsächlich benötigt, und mit der Anzahl der Geräte, die neu konfiguriert werden müssen. Dann erkennen Sie rasch, warum Netzwerkteams vor dem Einsatz von Automatisierung zurückschrecken.

Doch wiegen die Risiken der Netzwerkautomation wirklich schwerer als die Vorteile? Und können IT-Teams diese Risiken entschärfen? Sehen wir uns zunächst an, warum Unternehmen Netzwerkautomatisierung nutzen müssen und welche Risiken entstehen, wenn sie Automatisierung ignorieren.

WARUM TEAMS NETZWERKAUTOMATISIERUNG NUTZEN SOLLTEN

Standardisierte statt Snowflake-Designs. Komplexe Netzwerkdesigns – sogenannte Snowflake-Designs – bringen Risiken mit sich, weil ein Bereich des Netzwerks anders konfiguriert ist als ein anderer.

Das Fehlen von Standards erhöht das Risiko von Änderungen in allen Teilen des Netzwerks. Standardisierung ist einfach deshalb wichtig, weil das Netzwerk mit weniger – oder keinen – Spezialfällen zurechtkommen muss. Es kann besser Ausfallmodi

bestimmen und Standardverfahren für den Umgang mit ihnen entwickeln.

Standardisierte Bausteine für Netzwerkdesigns zu verwenden, macht Netzwerkautomatisierung einfacher. Das Equipment für Designs nach dem Baukastensystem mag etwas teurer sein, im Gegenzug ergeben sich aber geringere Betriebskosten und eine größere Resilienz. Durch die Nutzung von Standardverfahren für Fehlersuche und -behebung können Netzwerkteams Ausfälle leichter verstehen und beheben.

AUTOMATISIERUNG LÄSST SICH AM BESTEN EINFÜHREN, INDEM SIE MIT EINFACHEN AUFGABEN ANFANGEN.

Netzwerkdesigns, die auf standardisierten Bausteinen basieren, lassen sich viel einfacher automatisieren. Zur Automatisierungsunterstützung gehören Erstkonfiguration, Konfigurations-Updates, das Überprüfen der physischen Konnektivität und Troubleshooting.

Netzwerkagilität. Die Netzwerkautomation hinkt der Automatisierung von Compute- und Storage-Systemen hinterher und muss einiges aufholen. Unternehmen, die die Einführung einer vollständigen IT-Automatisierung verzögern, riskieren Nachteile gegenüber ihrer agileren Konkurrenz.

Automation heißt, dass die gesamte Organisation IT-Ressourcen effizienter nutzt. Effizienz führt zu Produktivität und höheren Gewinnen mit der gleichen Zahl an Mitarbeitern. Eine stabilere IT-Umgebung bedeutet mehr Stabilität für Kunden und größere Kundenzufriedenheit. Dies kann in vielen Fällen höhere Preise und einen größeren Marktanteil ermöglichen.

Darüber hinaus lässt sich ein agiles Netzwerk auch einfacher an neue Netzwerktechnologien anpassen. Das Netzwerkteam muss lediglich schrittweise Änderungen an einigen wenigen Bausteinen des Standarddesigns und an den damit verknüpften Automatisierungsaufgaben vornehmen.

RISIKEN DER NETZWERKAUTOMATISIERUNG

Bei der Einführung von Automatisierung bestehen allerdings ganz eigene Risiken. Jeder schlecht vorbereitete und schlecht implementierte Prozess kann das Netzwerk lahmlegen – und Automatisierung bildet keine Ausnahme.

Mit den folgenden Punkten können Netzwerkteams die Risiken durch Netzwerkautomatisierung verringern:

Beginnen Sie mit kleinen Schritten. Automatisierung lässt sich am besten einführen, indem Sie mit einfachen Aufgaben anfangen. Erstellen Sie zunächst einige einfache Skripte, die ein allgemeines Troubleshooting oder eine grundlegende Netzwerkanalyse durchführen, dabei aber nur lesend zugreifen. Das kann etwa die Suche nach einer bestimmten [MAC-Adresse](#) oder nach der [Root Bridge](#) in einer [Spanning-Tree](#)-Domäne sein. Sie sollten Such- oder Diagnoseaufgaben automatisieren, die häufig genutzt werden und die meiste Zeit beanspruchen. Nehmen Sie in dieser Phase

keine automatischen Änderungen vor. Konzentrieren Sie sich stattdessen darauf, die [Automatisierungs-Tools](#) kennenzulernen, die einen echten Mehrwert für den Netzbetrieb bringen.

Tests. Netzwerkautomatisierung muss denselben Prozess durchlaufen, den die Anwendungsentwicklung nutzt: intensive Tests. Anwendungsentwickler können rasch Server- und Client-VMs einrichten und umfangreiche Tests automatisiert durchführen. Im Gegensatz dazu sind Netzwerktests immer schon ein Problem gewesen, da Testlabore zu teuer waren und

ihre Einrichtung zu viel Zeit in Anspruch nahm.

Standarddesigns reduzieren die Anzahl der verschiedenen Varianten, die getestet werden müssen. Anbieter offerieren für viele Gerätetypen auch virtuelle Instanzen – häufig gegen eine kleine oder sogar ohne Gebühr, allerdings mit eingeschränkter Performance. Deshalb ist es wichtig, Konfigurationsänderungen auf diesen Geräten zu überprüfen.

Eventuell muss das Netzwerkteam mit dem Rest der IT zusammenarbeiten, um eine Testumgebung aufzubauen, die das





Home

Editorial

Überblick

Netzwerk-
Provisioning

Risiken und
Heraus-
forderungen

Tool-Auswahl

Performance
Monitoring

Dokumentation

Über die
Autoren

operative Netzwerk exakt widerspiegelt. Idealerweise enthält die Testumgebung Anwendungen und Test-Clients, um Netzwerk-Traffic zu generieren.

Netzwerkvalidierung. [Intent-based Networking](#) (IBN) ist der neueste Branchentrend, und Sie können mit IBN starten, indem Sie einige grundlegende Netzwerk-Checks erstellen. Das Überprüfen des Netzwerkstatus ist eine hervorragende Möglichkeit, Automatisierungsrisiken zu reduzieren.

Verifikation ist ebenfalls ein ausgezeichnetes Tool, wenn es darum geht, zu prüfen, ob Ihr Netzwerk wie vorgesehen funktioniert, sogar bevor Sie automatisierte Änderungen zulassen.

Um zu verifizieren, ob Ihr Netzwerk verbunden ist und wie gewünscht arbeitet, achten Sie auf den Netzwerkstatus. Dazu gehören der Status der Geräteschnittstelle, Adresszuweisung, benachbarte Geräte sowie Protokollinformationen auf [Layer 2 und Layer 3](#). In dieser Phase nehmen Sie keine Änderungen am Netzwerk vor. Das Intent-basierte Validierungsskript sollte einen Alarm auslösen, wenn ein Check fehlschlägt, so dass die Teams geeignete Gegenmaßnahmen ergreifen können.

Die Skripte zur Netzwerkvalidierung werden dann zu Tools, die Sie bei einem künftigen Änderungsprozess nutzen können, um Netzwerkvalidierungs-Checks vor und nach Änderungen

durchzuführen. Falls ein Validierungs-Check vor Änderungen fehlschlägt, nehmen Sie keine Änderungen vor.

Schlägt ein Validierungs-Check nach Änderungen fehl, alarmieren Sie die Netzwerkmitarbeiter und machen gegebenenfalls die Änderungen rückgängig. Achten Sie darauf, die Validierung vor Änderungen zu wiederholen, nachdem Sie die Änderung zurückgenommen haben. Auf diese Weise stellen Sie sicher, dass sich das Netzwerk wieder im Ausgangszustand befindet.

DAS ÜBERPRÜFEN DES NETZWERKSTATUS IST EINE HERVORRAGENDE MÖGLICHKEIT, AUTOMATISIERUNGSRISIKEN ZU REDUZIEREN.

ASPEKTE EINES ERFOLGREICHEN NETZWERKAUTOMATISIERUNG

Das wichtigste Konzept bei jedem System für Netzwerkänderungen besteht darin, Prozesse zu implementieren, die Risiken reduzieren.

Bei manuellen Anpassungen werden Change Control Boards und Review-Zyklen genutzt, und das wird weiter notwendig sein.

Doch Automatisierung wird zu zusätzlichen Prozessen führen, zum Beispiel zu einer automatisierten Validierung vor und nach Änderungen.

Falls Sie gerade erst mit Netzwerkautomation beginnen, beschränken Sie Ihre Arbeit auf Aufgaben, die nur lesend auf das Netzwerk zugreifen und es dadurch nicht beeinträchtigen. Das Wichtigste aber: Beginnen Sie jetzt! ■

Wie fängt man mit der Netzwerkautomatisierung an?

ALLES MÖGLICHST EINFACH HALTEN

Erstellen Sie einfache Skripte für die schreibgeschützte Fehlerbehebung oder Netzwerkanalyse.



TESTEN

Richten Sie eine Testumgebung ein, die dem operativen Netzwerk entspricht, einschließlich Anwendungen und Test-Clients.



VALIDIERUNG DURCHFÜHREN

Erstellen Sie grundlegende Netzwerkprüfungen, um sicherzustellen, dass das Netzwerk wie vorgesehen funktioniert.



QUELLE: TERRY SLATTERY; ICONS: TRETER/ADOBE STOCK

©2019 TECHTARGET. ALLE RECHTE VORBEHALTEN. 

DIE RICHTIGEN TOOLS FÜR DIE NETZWERKAUTOMATISIERUNG

Erstellen Sie eigene Skripte, wenn Sie Projekte zur Netzwerkautomatisierung starten? Oder kaufen Sie fertige Tools? Das Know-how Ihres Teams dürfte den Ausschlag geben. Von Dan Conde



ELENA/ADOBE

HOME

Netzwerkautomatisierung ist ein populäres Thema, doch IT-Fachleute sind angesichts der vielen Bedeutungen verwirrt. Damit kann die Automatisierung der Kommandozeile (Command Line Interface) mittels vorgefertigter Skripte in einer Sprache wie Python gemeint sein, um auf die [APIs](#) von Netzbetriebssystemen zuzugreifen. Automatisierung könnte aber auch mit der Nutzung von Software-defined Networks verbunden sein, die über einen Controller verwaltet werden.

Handelt es sich um Beispiele für [Netzwerkautomatisierung](#), und warum ist das wichtig? Der Großteil der IT-Infrastruktur – einschließlich Cloud- und traditioneller On-Premises-Systeme – ist dynamisch geworden. Aber die Netzwerke haben nicht Schritt gehalten. Deshalb wollen wir nicht, dass sie zu Bottlenecks werden.

Neidisch betrachten Unternehmen, wie große Cloud-Betreiber Software-defined Networking ([SDN](#)) anpassen, um ihre riesigen Netzwerke zu automatisieren, was jedoch für Unternehmen nicht praktikabel ist. Um eine höhere Agilität zu erreichen, könnten Organisationen Standardkomponenten in ihre SDN-Systeme implementieren, aber das dürfte für Unternehmen mit vorhandener Hardware nicht durchführbar sein.

Gibt es einfachere Möglichkeiten zu beginnen? CLI-basierte Skripte zu schreiben, ist eine vertraute, aber fehleranfällige Methode, die sich nicht gut skalieren lässt. Programme in Sprachen wie [Python](#) oder Ansible zu schreiben, um die APIs in modernen Netzwerkgeräten zu nutzen, ist ein guter Schritt im Hinblick darauf, Infrastruktur wie Code zu behandeln. Dieser

Home

Editorial

Überblick

Netzwerk-
ProvisioningRisiken und
Heraus-
forderungen

Tool-Auswahl

Performance
Monitoring

Dokumentation

Über die
Autoren

Ansatz dürfte die Kompatibilität mit bestehendem Equipment wahren und für Agilität via Automatisierung sorgen.

Ist das die ideale Kombination für Netzwerkautomatisierung – weder zu simpel noch technisch zu anspruchsvoll?

TOOLS ZUR NETZWERKAUTOMATISIERUNG: KOMPROMISSE

Als Ausgangspunkt für eine Netzwerkautomatisierung könnten Organisationen automatisierte Skripte von Vorlagen-Repositories herunterladen. Sie könnten einige Teile anpassen, um den Start zu erleichtern. Dieser Weg ist verlockend, wenn man ohne großen Aufwand rasche Erfolge verzeichnen will.

Programmieren kann auch Spaß machen. Das verbessert die [beruflichen Kompetenzen](#), und für die Ergebnisse kann es Lob geben. Gefährlich wird es allerdings, wenn darunter die eigentlichen Aufgaben Ihres Netzwerkteams leiden, etwa aufgrund von hohem Debugging-Aufwand. Sie wollen sicherlich nicht, dass durch das Programmieren die Netzwerkverwaltung ins Hintertreffen gerät.

An dieser Stelle müssen Sie Ihre Fähigkeiten einschätzen. Organisationen sollten sich darüber im Klaren sein, dass Netzwerkexperten nicht unbedingt zu Top-Programmierern mutieren. Training, Debugging- und Wartungsaufgaben werden leicht unterschätzt

und sind für Multi-Vendor-Umgebungen womöglich schwierig. Eine solche Strategie eignet sich vielleicht am besten für ein sachkundiges oder großes Team, das es sich leisten kann, genügend Ressourcen für diese Aufgabe bereitzustellen. Selbst wenn es für das Team funktioniert, denken Sie immer daran, dass bei dieser Herangehensweise Opportunitätskosten entstehen.

Alternativ können Anbieter oder Open-Source-Projekte Tools zur Verfügung stellen, die die Geräte-APIs nutzen, aber als fertiger Service verpackt sind. Das entlastet die Netzwerk-Profis davon, angepasste Skripte zu entwickeln. Hierbei handelt es sich um kein komplettes, vom Anbieter bereitgestelltes SDN-System, sondern um einen Service, der einer Skript-Automatisierungslösung von der Stange entspricht.

Das ist ein vernünftiger Kompromiss bei der Frage „Selbst machen oder kaufen?“. Ich empfehle dies für Organisationen, die einen Nachholbedarf in Sachen Automatisierung haben, es sich aber nicht leisten können, Ressourcen zu investieren, um Skripte anzupassen.

Die meisten modernen Netzwerkbetriebssysteme, zum Beispiel NX-OS von Cisco oder Junos OS von Juniper, verfügen über APIs, um das Scripting für Netzwerkautomatisierung

**SIE MÜSSEN IHRE
FÄHIGKEITEN EINSCHÄTZEN.
ORGANISATIONEN
SOLLTEN SICH DARÜBER
IM KLAREN SEIN, DASS
NETZWERKEXPERTEN
NICHT UNBEDINGT ZU TOP-
PROGRAMMIERERN MUTIEREN.**

[Home](#)[Editorial](#)[Überblick](#)[Netzwerk-Provisioning](#)[Risiken und Herausforderungen](#)[Tool-Auswahl](#)[Performance Monitoring](#)[Dokumentation](#)[Über die Autoren](#)

zu unterstützen. Die Produkte der Hersteller, wie Cisco DNA Center oder Juniper Contrail, bieten bereits fertige Services für die Netzwerkautomatisierung. Disaggregierte Netzwerkbetriebssysteme, etwa Cumulus Linux, und Automatisierungs-Tools von Drittanbietern, wie Apstra AOS, bieten ebenfalls diverse Formen herstellerunabhängiger Netzwerkautomatisierung.

BESTIMMEN SIE ZUERST IHRE ANFORDERUNGEN UND GESCHÄFTLICHEN ZIELE.

NETZWERKAUTOMATISIERUNG: EMPFEHLUNGEN

Bestimmen Sie zuerst Ihre Anforderungen und geschäftlichen Ziele. Organisationen mit komplexen Anforderungen können intern Programmier-Know-how zur Netzwerkautomatisierung aufbauen, wenn ein fertiger Service dafür nicht ausreicht. Wählen Sie diesen Ansatz aber nur, falls Sie die erforderlichen Fähigkeiten entwickeln und Experten anheuern können.

Für alle anderen eignen sich Standard-Tools für die Netzwerkautomatisierung, solange Sie sich der Einschränkungen bezüglich der Flexibilität bewusst sind. Ein hybrider Service ist möglich, aber Organisationen müssen die Grenzen eines fertigen Services verstehen und begreifen, wann ein angepasstes Skript sinnvoll ist. ■



[Home](#)[Editorial](#)[Überblick](#)[Netzwerk-
Provisioning](#)[Risiken und
Heraus-
forderungen](#)[Tool-Auswahl](#)[Performance
Monitoring](#)[Dokumentation](#)[Über die
Autoren](#)

Performance Monitoring in automatisierten Netzwerken

Virtuelle und automatisierte Netzwerke können oft Performance-Probleme verbergen. Nur mit der richtigen Performance-Monitoring-Strategie nutzen Sie diese Umgebungen optimal. Von [Andrew Froehlich](#)

Einige IT-Fachleute sind der Meinung, dass das Performance Monitoring von virtualisierten oder automatisierten Netzwerken sich nicht vom Monitoring traditioneller, hardwarebasierter Appliances unterscheidet. Das trifft allerdings keinesfalls zu.

Sowohl [Virtualisierung](#) als auch [Automatisierung](#) können leicht Probleme kaschieren, die eine Verschlechterung der Netzwerk-Performance verursachen.

Diese Probleme können völlig unbemerkt bleiben, wenn Admins herkömmliche [NPM-Tools](#) (Network Performance Monitoring) einsetzen.

Unternehmen, die die durch NPM-Analytics gewonnenen detaillierten Einblicke schätzen, erfahren im Folgenden alles

Notwendige über Monitoring in virtualisierten oder stark automatisierten Netzwerkinfrastrukturen.

**SOWOHL VIRTUALISIERUNG ALS
AUCH AUTOMATISIERUNG KÖNNEN
LEICHT PROBLEME KASCHIEREN,
DIE EINE VERSCHLECHTERUNG
DER NETZWERK-PERFORMANCE
VERURSACHEN.**

PERFORMANCE-MONITORING- STRATEGIE FÜR VIRTUELLE NETZWERKE

Obwohl Virtualisierung enorme Effizienz, [Skalierbarkeit](#) und Kosteneinsparungen bieten kann, hat sie auch einige Nachteile. Einer davon ist zusätzliche Komplexität. Das Troubleshooting von Legacy-Netzwerken, die auf [Bare-Metal](#)-Hardware-Appliances basieren, ist einfach, weil jeder Hop von einem Netzwerkgerät zum nächsten

eine physische Verbindung darstellt. Nun, da virtuelle Server die Regel sind, können Dutzende oder Hunderte von virtuellen



Home

Editorial

Überblick

Netzwerk-
Provisioning

Risiken und
Heraus-
forderungen

Tool-Auswahl

Performance
Monitoring

Dokumentation

Über die
Autoren

ES GEHÖRT ZWINGEND ZU PERFORMANCE- MONITORING-STRATEGIEN IN EINEM AUTOMATISIERTEN NETZWERK, DASS NUTZER DIE AUTOMATISIERUNGEN ÜBERWACHEN.

Maschinen ([VM](#)) auf einem einzigen Hypervisor laufen. Jede VM kann einen oder mehrere virtuelle Netzwerkadapter besitzen, die mit einem virtuellen Switch (vSwitch) verbunden sind. In einigen Fällen verfügt NPM-Software über wenig bis gar keine Sichtbarkeit in den vSwitch. Wenn eine VM mit einer anderen VM auf dem gleichen [Hypervisor](#) kommunizieren will, können einige NPM-Tools daher nicht den virtualisierten Layer durchdringen. Sollten Performance-Probleme bei diesem [vSwitch](#) auftreten, würden sich Netzwerkadministratoren schwertun, den Grund herauszufinden.

Die gute Nachricht ist, dass aktuellere Hypervisor die Sichtbarkeit in virtuelle Netzwerk-Appliances verbessert haben. Sie sollten aber überprüfen, ob Ihre NPM-Software und der vSwitch in der Lage sind, das erforderliche Maß an Sichtbarkeit zu gewährleisten.

Performance-Probleme können sich auch in der Hypervisor-Plattform oder in der physischen Hardware zeigen, auf der der Hypervisor läuft. Deshalb reicht es in virtualisierten Umgebungen nicht aus, einfach ein Monitoring innerhalb der VM durchzuführen – die Sichtbarkeit muss auch außerhalb der VM gegeben sein. Dazu gehört Performance Monitoring für den Hypervisor sowie für alle Computing-, Speicher- und Storage-Ressourcen.

Um die Sache noch komplizierter zu machen, lässt sich ein Hypervisor auch in einer verteilten Computing-Umgebung installieren. Das bedeutet: CPU, Speicher und Storage werden zugunsten einer verbesserten Effizienz und Skalierbarkeit für das Networking zusammengefasst.

Doch gleichzeitig mit diesen Vorteilen entsteht das Szenario von einem Netzwerk innerhalb eines Netzwerks. Die Geschwindigkeit Ihres IP-Netzwerks, das in einer VM läuft, kann aufgrund von Problemen im zugrunde liegenden

verteiltern Computing-Netzwerk plötzlich beeinträchtigt werden. Performance Monitoring für virtualisierte Netzwerkkomponenten bedeutet, auch die Performance von Hypervisor und verteilter Computing-Umgebung zu überwachen.

PERFORMANCE-MONITORING-STRATEGIE FÜR AUTOMATISIERTE NETZWERKE

Wenn alles funktioniert, kann Netzwerkautomatisierung eine ungeheure Zeitersparnis bedeuten. Läuft bei der Automatisierung aber etwas schief, kann das auch sehr schnell gehen.

Das zeigt sich etwa sehr gut daran, wie Automatisierung die Zuverlässigkeit von NPM negativ beeinflussen kann, wenn es darum geht, ein Performance-Problem schnell zu identifizieren und zu beheben. Ganz gleich, ob Sie einfache Skripte erstellen oder ein deutlich intelligenteres Automatisierungssystem

[Home](#)[Editorial](#)[Überblick](#)[Netzwerk-
Provisioning](#)[Risiken und
Heraus-
forderungen](#)[Tool-Auswahl](#)[Performance
Monitoring](#)[Dokumentation](#)[Über die
Autoren](#)

mithilfe von [Machine Learning](#) aufbauen: Automatisierung kann unbeabsichtigt zu Netzwerk-Performance-Problemen führen.

Obwohl dies ein separater Aspekt ist, wird das Problem durch den Umstand verschlimmert, dass Zeitaufwand und Komplexität, um das Problem zu identifizieren, deutlich steigen können, wenn die Automatisierungsprozesse selbst nicht richtig überwacht werden.

Wenn eine Person manuell Änderungen an der Netzwerk-konfiguration vornimmt, lässt sich einfach zurückverfolgen, wann und aus welchem Grund eine solche Änderung durchgeführt hat. Wenn also eine Änderung zu einem Netzwerk-Performance-Problem führt, kann der Administrator diese Änderung einfach rückgängig machen. Bei automatisierten Änderungen ist es nicht immer so leicht, zu ermitteln, wann oder warum die Änderung vorgenommen wurde. Daher stellen Sie und Ihre Nutzer möglicherweise eine verringerte Netzwerk-Performance fest, ohne zu wissen, wo deren Ursache liegt.

Es gehört zwingend zu Performance-Monitoring-Strategien in einem automatisierten Netzwerk, dass Nutzer die Automatisierungen überwachen. Deshalb ist ein gründliches Monitoring und Logging von allen automatisierten Änderungen ein wichtiger Bestandteil der Strategie. Auf diese Weise können Sie einen Abfall der Netzwerk-Performance leichter mit der Änderung korrelieren. Dies mag wie eine selbstverständliche Voraussetzung für Automatisierung erscheinen. Doch Sie wären überrascht, wie viele Administratoren diese Art der Protokollierung nicht auf die gleiche Stufe stellen wie die Notwendigkeit, die Netzwerk-Performance zu überwachen. ■

Monitoring für virtuelle und automatisierte Netzwerke

VIRTUELLE NETZWERKE

Überwachen Sie die Leistung virtueller Maschinen und der Hypervisor-Plattform. Vergessen Sie nicht, auch Rechen-, Memory- und Storage-Ressourcen zu überprüfen.

AUTOMATISIERTE NETZWERKE

Überwachen und protokollieren Sie alle Automatisierungsprozesse und -änderungen. Auf diese Weise können Netzwerkteams potenzielle Probleme bei der Netzwerkleistung besser erkennen.



ILLUSTRATION: APINAN/ADOBE STOCK; ©2019 TECHTARGET. ALLE RECHTE VORBEHALTEN.

Dokumentation zur Netzwerkautomatisierung

Ohne ordnungsgemäße Dokumentation kann die Netzwerkautomatisierung Unternehmen mehr Probleme als Vorteile bringen. Diese vier Überlegungen helfen bei der Netzwerkdokumentation. Von [Andrew Froehlich](#)

Die Netzwerkautomatisierung kann Netzwerkteams helfen, Zeit zu sparen. Doch wenn das Projekt nicht ausreichend dokumentiert ist, kann es auch zur Katastrophe kommen.

Eine korrekte [Dokumentation von Netzwerken](#) erfordert einige wenige Punkte, damit Teams den größten Nutzen daraus ziehen können.

1. Tiefes Verständnis für manuelle und automatisierte Prozesse. Netzwerkteams sollten einen umfassenden Überblick über den manuellen Prozess haben, den die Automatisierung ersetzen wird. Dieser Überblick bringt Sie zum Kernziel der Netzwerkautomatisierung. Jede größere Änderung, die einen manuellen Prozess verändern könnte, würde auch Änderungen im automatisierten Prozess erfordern. Netzwerkteams sollten die Dokumentation der Netzwerkautomatisierung wieder auf die manuellen Schritte zurückführen.

2. Detaillierte Dokumentationsproben. Teams sollten Code- oder Konfigurationsproben mit detaillierten Hinweisen zum

Was und Warum des Prozesses zur Verfügung stellen. Wenn die Dokumentation eine Überprüfung erfordert, bedeutet dies wahrscheinlich eine der folgenden Maßnahmen:

- Der automatisierte Prozess ist unterbrochen.
- Eine Änderung im Netzwerk erfordert eine Änderung der manuellen und automatisierten Prozesse.
- Ein auftretendes Hinzufügen erfordert eine Änderung der manuellen und automatisierten Prozesse.

In allen drei Situationen wird der für Hinzufügungen und Änderungen zuständige Automatisierungsingenieur wahrscheinlich mehr von Code-Proben profitieren als von generischen Erklärungen der automatisierten Aufgaben.

3. Konsistentes Vokabular in allen Dokumenten. Die IT-Teams sollten sicherstellen, dass die gesamte Dokumentation von Netzwerken die gleiche Terminologie und Nomenklatur verwendet, um Prozesse, Komponenten und Aufgaben zu beschreiben, die die Automatisierungskonfigurationen ersetzen.

Bei Bedarf können Netzwerkteams ein Glossar für die Automatisierungsdokumentation erstellen, das alle verwendeten Begriffe und Definitionen auflistet. Die Teams sollten auch dieses Dokument pflegen.

4. Leicht zugängliche Netzwerkdokumentation. Schließlich sollten die Netzwerkteams sicherstellen, dass die gesamte Dokumentation zur Netzwerkautomatisierung zentralisiert, zugänglich und bearbeitbar ist für diejenigen, die die

EINE KORREKTE DOKUMENTATION VON NETZWERKEN ERFORDERT EINIGE WENIGE PUNKTE.

Dokumentation benötigen. Wenn ein Benutzer Änderungen oder Ergänzungen vornimmt, sollten die Teams die Dokumentation [aktualisieren](#) und auf ihre Richtigkeit überprüfen.

Der beste Weg, diese Zugänglichkeit zu erreichen, ist der Einsatz von Tools für Enterprise Change Control Management. Diese Tools können dazu beitragen, dass die Dokumentation regelmäßig aktualisiert wird. ■



Home

Editorial

Überblick

Netzwerk-
Provisioning

Risiken und
Heraus-
forderungen

Tool-Auswahl

Performance
Monitoring

Dokumentation

Über die
Autoren

JESSICA SCARPATI ist eine in Boston ansässige freiberufliche Journalistin. Sie ist die ehemalige Feuilleton- und E-Zine-Redakteurin für die Networking Media Group von TechTarget.

AMY LARSEN DECARLO arbeitet seit über 17 Jahren in der IT-Industrie und ist leitende Analystin bei Current Analysis. Dort liegt der Fokus ihrer Untersuchungen auf der Bewertung gemanagter und Cloud-basierter Data Center sowie Security Services.

TERRY SLATTERY ist Principal Architect beim Netzwerkberatungsunternehmen NetCraftsmen. Er arbeitet an Netzwerkmanagementaufgaben, einschließlich software-definierte Netzwerk- und Business-Strategie-Beratung. Terry Slattery ist der Gründer von Netcordia, einem Netzwerkkonfigurations-Management-Unternehmen.

DAN CONDE ist IT-Analyst und Berater. Er war zuvor Analyst bei der Enterprise Strategy Group (ESG), wo er sich mit Technologien für Unternehmensnetzwerke beschäftigte.

ANDREW FROELICH ist seit über 15 Jahren in der Unternehmens-IT tätig. Sein Hauptaugenmerk galt Cisco-Technik (LAN und WLAN sowie Design von Sprachnetzwerken).

ComputerWeekly.de



Einstieg in die Netzwerkautomatisierung
ist eine Publikation von ComputerWeekly.de

Michael Eckert | Editorial Director

Malte Jeschke | Senior Online Editor

Ulrike Riess | Senior Online Editor

Tobias Wendehorst | Senior Online Editor

Franziska Holzfurtner | Trainee

Becky Wrigley | Production Editor

Brent Boswell | Herausgeber

BBoswell@techtarget.com

Hauptsitz:

TechTarget, 275 Grove Street, Newton, MA 02466

www.techtarget.com

Deutsche Redaktion:

TechTarget Deutschland, Landwehrstraße 61, 80336 München

www.techtarget.de

© 2020 TechTarget Inc. Kein Teil dieser Veröffentlichung darf ohne vorherige schriftliche Genehmigung des Verlages in irgendeiner Form oder auf irgendeine Weise weitergegeben oder reproduziert werden. Nachdrucke von TechTarget-Publikationen sind verfügbar über The YGS Group.

Über TechTarget: TechTarget publiziert Informationen für Profis im Bereich Informationstechnologie. Mehr als 100 Themen-Websites ermöglichen schnellen Zugriff auf ein reichhaltiges Angebot an Nachrichten, Ratgebern und Analysen über die Technologien, Produkte und Prozesse, die entscheidend sind für beruflichen Erfolg. Unsere Live- und virtuellen Veranstaltungen vermitteln direkten Zugang zu den Einschätzungen und Ratschlägen unabhängiger Experten. IT Knowledge Exchange, unsere soziale Community, bietet die Möglichkeit, um Rat zu fragen und sich mit Kollegen und Experten über Lösungen auszutauschen.