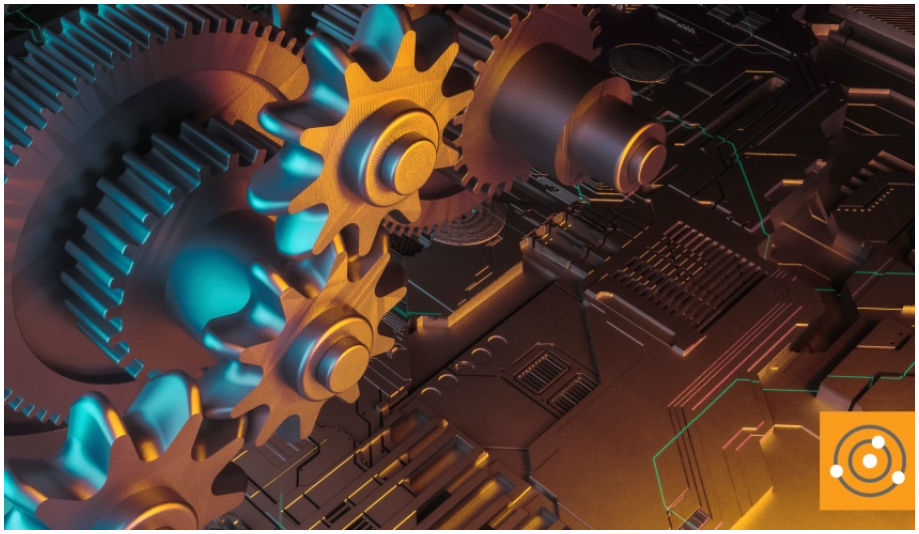
Im Test: SolarWinds Network Configuration Manager 2019.4 HF1

Leistungsstarkes Frontend zur Konfiguration von Netzwerkkomponenten

Dr. Götz Güttich

Mit dem Network Configuration Manager bietet SolarWinds ein Werkzeug an, mit dem sich die Konfigurationen von Netzwerkkomponenten wie Firewalls, Load Balancern, Routern, Switches und WLAN-Access Points an einer zentralen Stelle verwalten und bearbeiten lassen. Das Tool hilft beim Automatisieren der Administration, beim Herstellen der Compliance, beim Vulnerability Assessment und beim Erstellen von Konfigurations-Backups. Wir haben uns im Testlabor angesehen, was die Lösung in der Praxis zu leisten imstande ist.



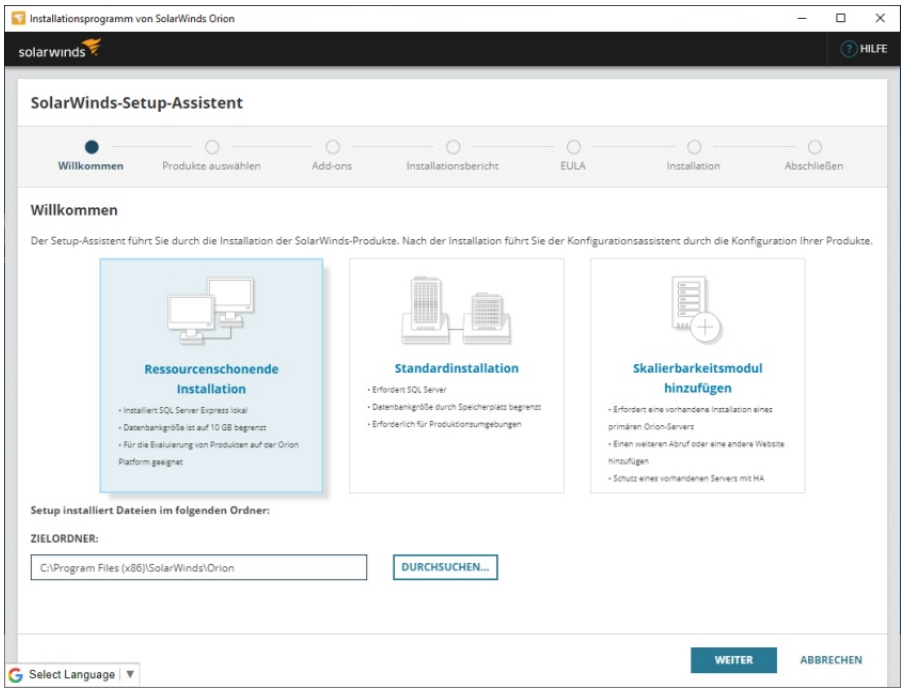
Der Network Configuration Manager (NCM) von SolarWinds ist nicht nur dazu in der Lage, die oben erwähnten Arbeiten durchzuführen, sondern kann auch beim Verwalten der Firmware-Updates helfen und das Device Lifecycle Management unterstützen. Damit sorgt die Lösung dafür, dass die IT-Mitarbeiter Zeit sparen, die Verfügbarkeit der Netzwerkdienste verbessern, Risiken minimieren und den Netzwerksstatus besser im Auge haben. Mit dem NCM werden die IT-Verantwortlichen in die Lage versetzt, Konfigurationsfehler zu finden, Skripts einzusetzen und ihre Konfigurationen in Archiven zu verwalten.

Die Lösung bietet sogar Funktionen zum Vergleichen von Konfigurationen an, die zeigen, was wann verändert wurde und Rollbacks ermöglichen. Im Betrieb durchsucht der NCM das Netz nach den entsprechenden Komponenten, lädt die Konfigurationen herunter und sichert sie in einer zentralen Datenbank. Die genannten Skripts lassen sich regelmäßig auf einzelnen oder auch mehreren Geräten durchführen, was manuelle Arbeiten zu großen Teilen überflüssig macht und damit auch eine große Fehlerquelle beseitigt. Umfassende Überwachungsfunktionen sorgen gleichzeitig dafür, dass stets Klarheit über den Zustand der einzelnen Geräte herrscht. Dazu kommen leistungsfähige Berichte und Alarmfunktionen, die die zuständigen Mitarbeiter jederzeit über auftretende Probleme, wie beispielsweise unerwünschte Konfigurationsänderungen, informieren. Im Betrieb kommt der NCM mit praktisch allen Netzwerkgeräten zurecht, die über ein textbasiertes Konfigurationsinterface verfügen. Dazu gehören unter anderem Produkte von Adtran, Agilent, Arris, Aruba, Cisco, Dell, Extreme, F5, Foundry, HP, Juniper, Marconi, Motorola, Netscaler, Netscreen, Nortel und Radware. Aus Sicht des Administrators macht es dabei keinen Unterschied, ob er ein oder 100 oder mehr Geräte verwaltet, da die Arbeitsschritte immer die gleichen sind.

Aufbau des Systems

Der NCM setzt auf der Orion-Plattform auf, SolarWinds zentra-

lem Werkzeug für Alerts, Reporting und Management. Als Betriebssystem setzt das System den Windows Server 2016 oder den Windows Server 2019 voraus, zum Testen lässt sich die Software aber auch auf Windows 8.1- oder Windows 10-Maschinen einspielen. Auf Hardwareseite erwartet die das Produkt einen Dual-Core-Prozessor mit drei GHz Taktfrequenz, sechs GByte RAM und 30 GByte freien Festplattenplatz. Darüber hinaus sollten der IIS 8 oder neuer, die ASP .NET 2.0 Ajax Extension 1 oder neuer sowie das .NET-Framewort 4.8 auf dem Zielsystem vorhanden sein.



Der Setup-Wizard kommt übersichtlich daher

Abgesehen davon benötigt die Lösung noch eine Datenbank. Für Testzwecke kann das der mitgelieferte Microsoft SQL Server Express 2017 sein, für Produktivumgebungen sollte ein "richtiger" SQL Server oder die Azure SQL Database zum Einsatz kommen.

Alternativ kann das System in der öffentlichen oder einer privaten Cloud installiert werden und befindet sich auch im Microsoft Azure Marketplace. An Browsern unterstützt der NCM den Internet Explorer 11, Microsoft Edge, Firefox 49 oder neuer sowie Chrome 54 oder neuer.

Der Test

Im Test spielten wir den NCM in unserem Netzwerk ein und machten uns mit dem Funktionsumfang der Lösung vertraut. Anschließend arbeiteten wir mit dem Produkt, veränderten Konfigurationen mit Hilfe von Skripts, setzten Templates ein und nahmen insbesondere die Funktionen zum Überwachen von Konfigurationsänderungen mit Alarmmeldungen via E-Mail und die Features zum Sicherstellen der Compliance unter die Lupe. Außerdem befassten wir uns auch mit der Thematik der Firmware-Upgrades.

Installation

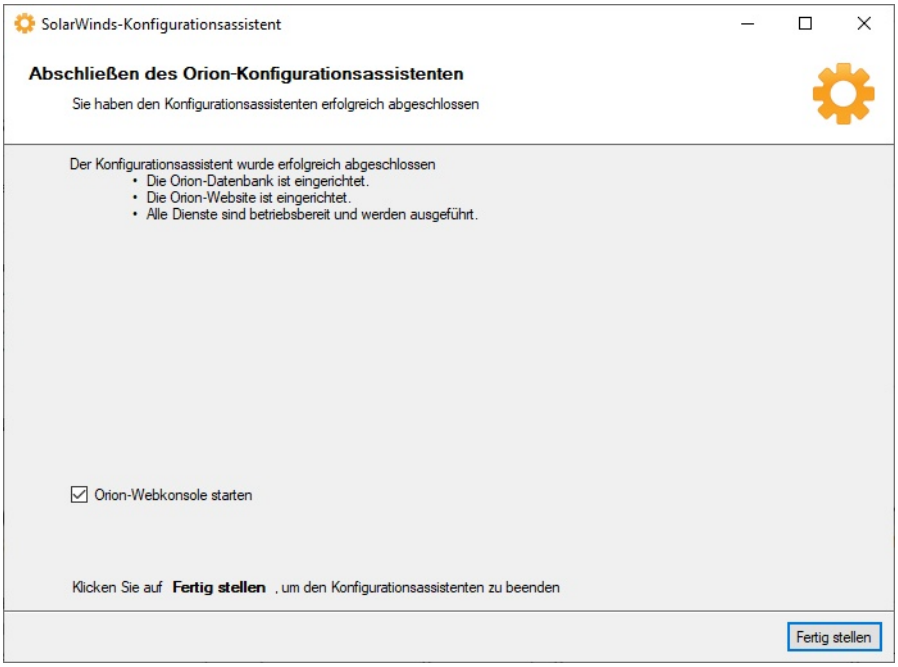
Für die Installation des NCM luden wir uns zunächst einmal von der Webseite des Herstellers die entsprechende Setup-Datei herunter und starteten diese mit einem lokalen Administratorkonto. Als Server verwendeten wir im Test übrigens einen Windows Server 2019 mit einer Intel i7-CPU mit 3,6 GHz Taktfrequenz, acht GByte RAM und 120 GByte freiem Festplattenplatz. Als Datenbank setzten wir ein Microsoft SQL Server 2017-System ein, das sowieso schon in unserem Netz seinen Dienst versah.

Nach dem Aufruf des Installers spielte dieser erst einmal das .NET 4.8-Framework ein und verlangte dann einen Neustart. Danach bot uns die Installationsroutine die Wahl zwischen einer ressourcenschonenden Installation mit einer auf dem SQL Server Express basierenden Datenbank mit einer Maximalgröße von zehn GByte (die sich zum Testen der Lösung eignet) und einer Standard-Installation mit einem externen SQL Server, bei der es dann keine Größenbeschränkung der Datenbank gibt. In unserer Umgebung entschieden wir uns für die Standard-Installation.

Im nächsten Schritt fragte uns der Setup-Wizard, ob wir auch den Orion Log Viewer einspielen wollten, der als Datenbank mindestens einen SQL Server 2016 mit Service Pack 1 voraussetzt. Da wir ja einen SQL Server 2017 verwendeten und den gesamten Funktionsumfang der Lösung testen wollten, entschieden wir uns an dieser Stelle für „Ja“. Nun zeigte uns der Installer Lizenzinformationen an und lud dann die einzuspielenden Software-Pakete herunter und installierte sie. Als das erledigt war, startete der Assistent zur Erstkonfiguration und fragte uns nach der zu verwendenden Datenbank. Sobald die Verbindung zum SQL Server her-

gestellt war, bot uns der Assistent an, eine neue Datenbank anzulegen oder eine bestehende zu nutzen. Im Test legten wir eine neue an. Dabei mussten wir noch das für die Datenbank einzusetzende Konto angeben.

Jetzt ging es an die Konfiguration der Web-Konsole mit dem zu verwendenden Port und der SSL-Verschlüsselung und die Auswahl der zu installierenden Dienste. Zum Schluss mussten wir noch



Das System nach dem Abschluss des Setups

angeben, ob wir eine getrennte Datenbank für die Protokoll- und Ereignisüberwachung anlegen wollten (das wollten wir), danach war die Erstkonfiguration abgeschlossen und wir konnten mit dem System arbeiten. Das ganze Setup lief demzufolge recht unkompliziert ab und sollte keinen IT-Verantwortlichen vor Probleme stellen.

Erste Schritte mit dem NCM

Wenn man sich zum ersten Mal als Administrator beim Web-Portal der Lösung anmeldet, muss man direkt sein Passwort anpassen. Das ist sehr gut, denn so verhindert SolarWinds, dass Installationen mit einem Standard-Passwort im Netz zum Einsatz kommen.

Nachdem wir unser Passwort gesetzt hatten, spielten wir zunächst einmal über das Web-Interface die Lizenz ein, die uns der Hersteller zur Verfügung gestellt hatte. Danach ging es daran, die zu verwaltenden Knoten zu unserer Testumgebung hinzuzufügen. Dazu haben die Anwender zwei Möglichkeiten: Zum einen können sie den NCM das Netz durchsuchen lassen und die gefundenen Geräte automatisch hinzufügen, zum anderen besteht auch die Option, die Knoten manuell anzugeben, was bei wenigen zu verwaltenden Komponenten der sinnvollere Weg ist. Da wir zu diesem Zeitpunkt nur ein zu konfigurierendes Testgerät in unserer Umgebung hatten (einen Cisco-Switch vom Typ WS-C2960C-8TC-S), fügten wir dieses manuell zum NCM hinzu. Dazu gaben wir zunächst die Community-Namen für die schreibgeschützten und mit Lese- beziehungsweise Schreibzugriff versehenen SNMP-Communities an. Danach erschien das Gerät in der Liste der verwalteten Komponenten.

Um es auch über die NCM zu steuern, wechselten wir danach nochmals in die Eigenschaften des Switches und hinterlegten dort ssh-Zugangsdaten. Jetzt konnten wir die Komponente auch mit dem NCM administrieren. Im Prinzip kann man die beiden Schritte mit den SNMP- und SSH-Zugangsdaten auch auf einmal erledigen, es sind also nicht unbedingt zwei Konfigurationsschritte erforderlich. Natürlich müssen die zu verwaltenden Geräte zuvor so konfiguriert sein, dass sie per SNMP und SSH ansprechbar sind, das dürfte aber in den meisten Umgebungen der Fall sein. NCM unterstützt übrigens als Zugriffsprotokoll auch Telnet, was in manchen Umgebungen aus Kompatibilitätsgründen von Vorteil sein kann. Nachdem alles zu unserer Zufriedenheit lief, machten wir uns zu diesem Zeitpunkt daran, ein paar grundlegende Tätigkeiten mit dem NCM durchzuführen, um uns mit seiner Oberfläche und dem Bedienkonzept zu befassen. So setzten wir uns zunächst einmal mit Skripts und Templates auseinander.

Arbeit mit Skrips wie auf der Kommandozeile

Die Skripts lassen sich beliebig definieren und können auf einem oder mehreren Geräten im Netz laufen. Wenn ein IT-Mitarbeiter genau weiß, welche Konfigurationsänderungen er durchführen will und wie die dazugehörige Syntax lautet, so sind Skripts die richtige Wahl. Über Skripts besteht unter anderem die Option,

Aufgaben wie das Herunterladen von Konfigurationsdateien, das Aktualisieren von ACLs oder auch das Verändern von Login-Bannern durchzuführen.

Im Test fingen wir klein an, und modifizierten zunächst einmal das Login-Banner unseres Switches mit Hilfe eines Skripts. Dazu wechselten wir zunächst im Konfigurationsinterface nach „Meine Dashboards / Netzwerkkonfiguration / Configuration Management“ und klickten auf den „Script Management“-Reiter. Anschließend wählten wir den Befehl „Add New Script“ aus. Daraufhin öffnete sich ein Editor mit nummerierten Zeilen, in dem wir unser Skript eintragen konnten. Nachdem wir es komplettiert und abgespeichert hatten, konnten wir es über den Befehl "Execute Script" direkt ausführen. Dieser fragt zuerst, auf welchen Geräten das Skript laufen soll und möchte dann wissen, welches Skript zu starten ist. Anschließend führt er das Skript dann aus. Im Test traten dabei keinerlei Probleme auf.

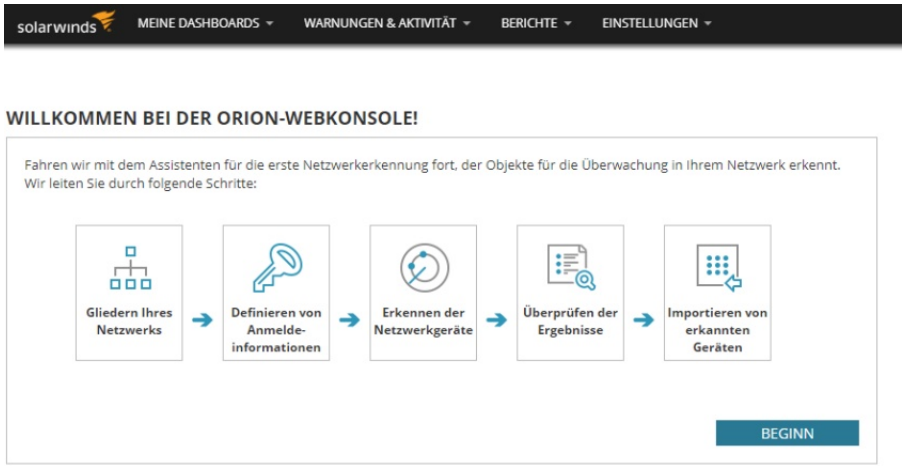
Den Überblick behalten mit der Inventory-Funktion

Um detaillierte Informationen über die verwendeten Geräte zu erhalten, stellt der NCM eine umfassende Inventory-Funktion bereit. Diese sammelt Daten über die Modelle und Seriennummern, die verwendeten Betriebssystemversionen, die Zahl der Netzwerkanschlüsse sowie Routing-Protokolle, IP-Adressen, aktive Ports und ähnliches. Die Inventories stellen die Grundlage für Konfigurationsänderungen aufgrund von Templates dar (zu den Templates, also den Vorlagen für automatisch erzeugte Skripts, gleich mehr). Die IT-Verantwortlichen müssen demzufolge immer einen Inventory-Scan ihrer Geräte durchführen, bevor sie mit Templates arbeiten können. Erst nach einem solchen Scan weiß das System beispielsweise wie viele Ports ein Switch hat und wie sie konfiguriert sind. Nur mit diesen Informationen lassen sich die Templates mit sinnvollen Werten ergänzen und automatisch Skripts generieren.

Die Daten, die die Inventory-Scans sammeln, können zusätzlich auch in Reports einfließen. Die Scans lassen sich entweder über alle Nodes hinweg, über Node-Gruppen oder über einzelne Nodes durchführen. SolarWinds empfiehlt in diesem Zusammenhang einen täglichen Inventory-Scan über alle Systeme hinweg in der Nacht. Bei Bedarf sind die Administratoren aber auch in der Lage, die Scans manuell anzustoßen, und zwar unter "Meine Dashboards / Netzwerkkonfiguration / Configuration Management". Dort wählen sie das jeweils betroffene Gerät aus und klicken dann auf "Update Inventory". Im Test führten wir zu diesem Zeitpunkt einen Scan durch und erstellten anschließend einen Inventory Report, um die Ergebnisse einzusehen. Dabei traten keine Überraschungen zu Tage. Auf die Reports gehen wir später auch noch genauer ein.

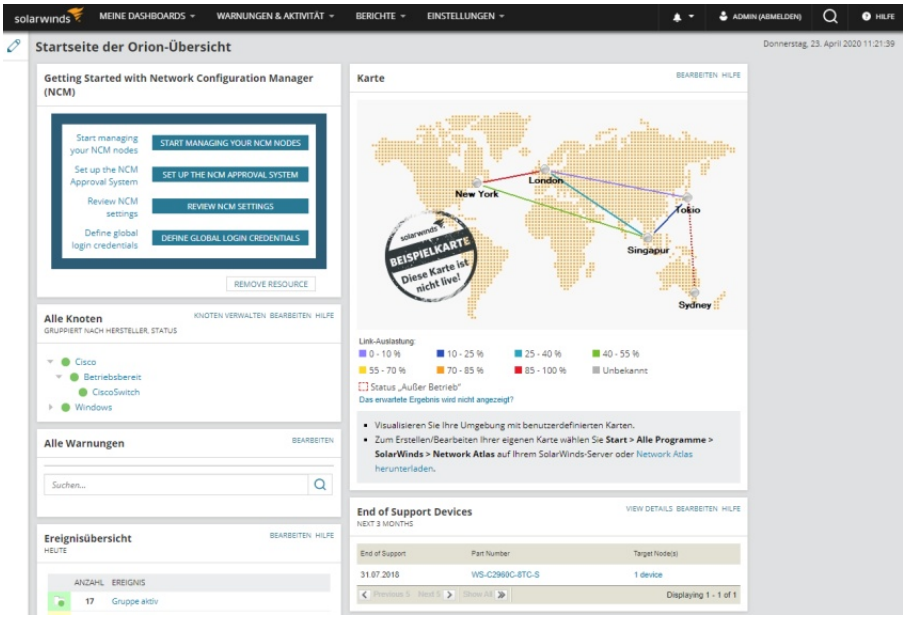
Flexibles Arbeiten mit Templates

Nachdem wir unsere Umgebung inventarisiert hatten, konnten wir uns mit den eben genannten Templates auseinandersetzen. Wie der Name schon vermuten lässt, handelt es sich dabei um Vorlagen, mit denen sich typische Konfigurationsaufgaben automatisiert abarbeiten lassen. SolarWinds stellt im Rahmen des NCM 48 Templates, geordnet nach Herstellern und Aufgabengebieten, also beispielsweise 12 Templates für Cisco, 19 Templates für Lenovo, drei NetFlow-Templates und so weiter, bereit. Es ist auch möglich, eigene Templates zu erstellen und über die Web-Plattform "THWACK" (https://thwack.solarwinds.com) Templates mit anderen Nutzern auszutauschen. Dort befinden sich hunderte weiterer Vorlagen für die verschiedensten Aufgaben oder Hersteller zum Download. Typische Aufgaben, für deren Erledigung sich Templates eignen, sind das Anpassen von SNMP-Einstellungen, das Ändern von Passwörtern, das Definieren von ACLs und das Modifizieren von VLAN-Mit-



Ein Wizard hilft bei der Erstkonfiguration

gliedschaften. Im Test machten wir uns jetzt daran, einen der Switch-Ports in unserem Cisco-Switch einem anderen VLAN zuzuordnen. Dazu wechselten wir zunächst einmal nach "Meine Dashboards / Netzwerkkonfiguration / Config change templates" und selektierten dort im Menüpunkt "Cisco" das Template „Change VLAN Membership on Ports Cisco IOS“. Anschließend klickten wir auf den Befehl "Define Variables & Run", wählten



Die Startseite des NCM-Web-Interfaces

das Zielsystem aus (auch hier lassen sich wieder beliebig viele Zielsysteme gleichzeitig angeben) und legten dann fest, welcher Port welchem VLAN zugewiesen werden sollte. Anschließend konnten wir uns im Web-Interface das Skript ansehen, das der NCM mit unseren Angaben auf dem Zielsystem ausführen würde und den Vorgang danach mit "Execute" starten. Auch hier traten im Test keine Probleme auf. Die Templates sind als besonders positives Feature hervorzuheben. Sie versetzen nämlich nicht nur erfahrene Administratoren dazu in die Lage, effizient mit ihren Netzwerkkomponenten zu arbeiten, sondern ermöglichen es auch IT-Mitarbeitern – die beispielsweise keine genaueren Kenntnisse mit den Kommandozeilenbefehlen von Cisco-Lösungen haben – viele grundlegende Verwaltungstätigkeiten durchzuführen, da die SolarWinds-Lösung die auszuführenden Skripts ja anhand der Vorlagen selbst erstellt. Damit lassen sich in den IT-Abteilungen viele Standard-Arbeiten auf mehrere Schultern verteilen und so die Effizienz erhöhen.

Das Verwalten von Konfigurationsänderungen

Nachdem wir nun mit Skrips und Templates ein paar Konfigurationsänderungen durchgeführt hatten, konnten wir uns mit dem Konfigurationsmanagement des NCM auseinandersetzen. Unter "Meine Dashboards / Netzwerkkonfiguration / Config Summary" findet sich unter anderem eine Übersicht mit den letzten fünf Konfigurationsänderungen mit dem betroffenen Netzwerk-Node und dem Datum. Über einen Klick lässt sich nun ein so genannter Change Report aufrufen, der die Konfiguration vor und nach der Änderung zeigt und die Modifikationen farblich hervorhebt. So sehen die zuständigen Mitarbeiter sofort, was auf ihren Systemen vorgeht. Auch Fehler lassen sich auf diese Weise einfach finden.

Eine Änderung rückgängig machen

Kommt es nach der Modifikation der Konfiguration eines Systems zu Problemen, so ist es oft der schnellste und einfachste Weg, diese Änderung einfach rückgängig zu machen. Der NCM unterstützt dieses Vorgehen durch einen Klick auf den betroffenen Node und die Auswahl des Reiters "Configs". Anschließend kann er unter „Upload Configs“ eine zuvor verwendete Konfiguration hochladen und das System so wieder in den vorherigen Zustand versetzen.

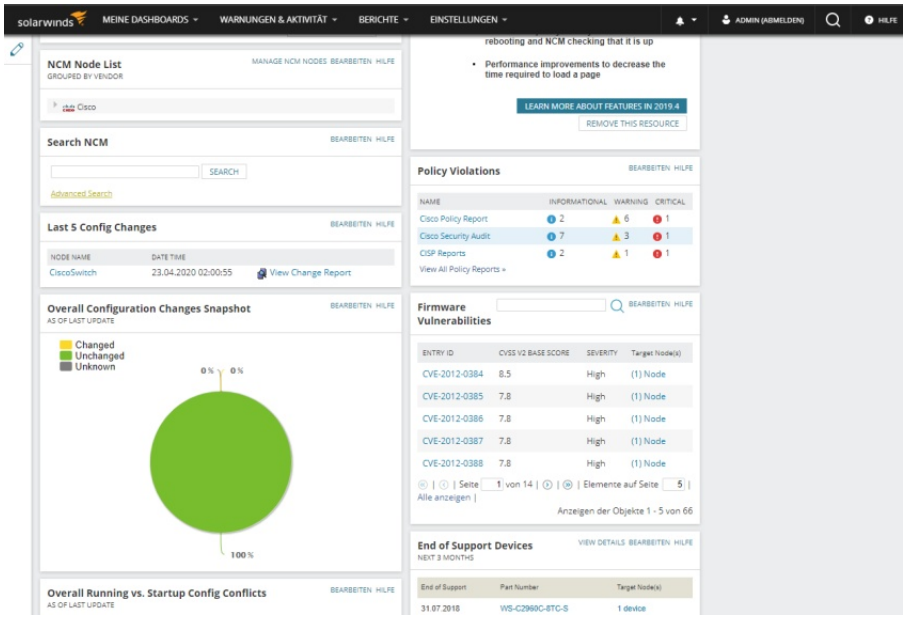
Konfigurationsbackups sollten regelmäßig stattfinden

Im Betrieb ist es nicht nur wichtig, die Konfigurationsänderungen im Blick zu behalten, sondern auch regelmäßige Backups der Konfigurationen anzulegen, damit die IT-Verantwortlichen dazu in der Lage sind, jederzeit Rollbacks zu vorher definierten Punkten durchzuführen. Standardmäßig erstellt der NCM jede Nacht ein Backup der Konfigurationen der verwalteten Geräte. Im Test funktionierte das einwandfrei. Bei Bedarf lässt sich dieser Zeitplan aber beliebig an die Anforderungen der jeweiligen Umgebung anpassen. Die Backups lassen sich bei Bedarf auch automatisch immer dann sichern, wenn eine Änderung vorgenommen wurde, was wohl in den meisten Umgebungen sinnvoll sein dürfte. SolarWinds empfiehlt auf jeden Fall, mindestens einmal pro Woche ein Backup anzulegen.

Bei Bedarf ist es auch möglich, jederzeit manuell ein Backup zu erzeugen. Dazu müssen die zuständigen Mitarbeiter lediglich nach "Meine Dashboards / Netzwerkkonfiguration / Configuration Management" wechseln und das betroffene Gerät auswählen. Nach einem Klick auf "Download / Running" oder "Download / Startup" lädt der NCM die entsprechende Konfiguration herunter.

Die Überwachung von Konfigurationsänderungen

Wenden wir uns zu diesem Zeitpunkt zwei echten Highlights des NCM zu: Der sofortigen Meldung von Konfigurationsänderungen und der Sicherstellung der Geräte-Compliance. Fangen wir mit der Meldung der Konfigurationsänderungen an. Wendet ein Administrator eine komplexe Konfigurationsänderung an, beispielsweise indem er auf mehreren Switches die VLAN-Zugehörigkeit unterschiedlicher Ports modifiziert, kann das bei einer Fehlkonfiguration dazu führen, dass eine Vielzahl an Diensten im Netz ausfallen. In so einem Fall ist es von großem Nutzen, wenn die zuständigen Mitarbeiter über die auftretenden Schwierigkeiten informiert werden, bevor die Ausfallzeiten so zunehmen, dass sie die Produktivität des Unternehmens beeinträchtigen. Deswegen bietet der NCM die Möglichkeit, Administratoren per E-Mail über aktuelle Probleme zu informieren. Dieses Feature nennt sich "Real Time Detection" und funktioniert mit Netzwerkkomponenten, die dazu in der Lage sind, bei Konfigurationsänderungen SNMP-Traps oder Syslog-Meldungen zu verschicken. Auf unserem Cisco-Testsystem konnten wir im Test die Konfiguration des Geräts einfach so anpassen, dass es Syslog-Nachrichten verschickte. Dazu mussten wir lediglich das NCM-Template "Enable Syslog – Cisco OS" darauf laufen lassen. Dieses wollte nur die IP-Adresse des Syslog-Servers – in diesem Fall



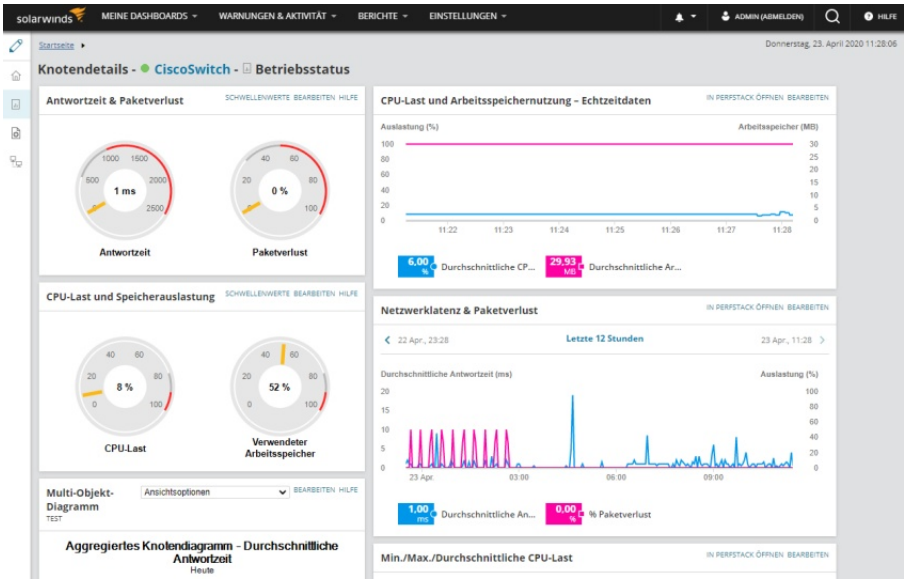
Die Konfigurationsübersicht zeigt unter anderem Policy-Verletzungen und Firmware-Vulnerabilities

des NCM-Servers – und den Log-Level wissen, danach lief es anstandslos durch.

Auf der Empfängerseite verwendet der NCM einen eingebauten SNMP-Trap-Receiver und Syslog-Server. Dabei erkennt eine Syslog-Regel die Konfigurationsänderungen und informiert anschließend die Administratoren. Um diese Syslog-Regel einzurichten, müssen sich die zuständigen Mitarbeiter als Administratoren beim NCM anmelden und im SolarWinds-Programmordner unter „Program Files (x86)\Solarwinds\Orion“ den "Syslog Viewer" aufrufen. Dabei handelt es sich um eine Windows-Anwendung, die unter "View / Alerts/Filter Rules" die Möglichkeit bietet, die vordefinierte NCM-Regel "Cisco IOS Realtime Change Notifications" zu aktivieren. Jetzt ist es nur noch erforderlich, die Real Time Detection im NCM-Web-Interface zu starten. Das geht unter "Einstellungen / Alle Einstellungen / Produktspezifische Einstellungen / NCM Einstellungen". Dort existiert der Eintrag "Real-Time Change Detection", der sich an gleicher Stelle auch konfigurieren lässt.

Dazu gaben wir zunächst einmal auf der Konfigurationsänderungsseite an, dass wir zusammen mit der E-Mail auch die auslösende Syslog- beziehungsweise Trap-Nachricht erhalten wollten. Danach wechselten wir auf die "Config Download and Notification Settings"-Seite, gaben die E-Mail-Adresse an und klärten, ob wir die laufende oder die Startkonfiguration überwachen wollten und mit welcher Konfiguration wir diese vergleichen wollten (Baseline Config oder der letzten heruntergeladenen Konfigurationsdatei). Hier sieht man schon, dass die Funktion sehr leistungsfähig ist und sich flexi-

bel an die jeweiligen Bedürfnisse anpassen lässt. Zum Abschluss der Konfiguration mussten wir nur noch den zu verwendenden SMTP-Server angeben und die Real Time Config Change-Funktion aktivieren. Danach funktionierte alles wie erwartet und die Alert-Mails, die man erhält, enthalten auch gleich einen direkten Link zur festgestellten Konfigurationsänderung.



Der Betriebsstatus unseres Switches mit umfassenden Informationen

Das Sicherstellen der Compliance

Ein weiteres Highlight des NCM ist die Möglichkeit, die Compliance der im Netz verwendeten Geräte auf eine einfache Art und Weise sicher zu stellen. Dazu stellt das Werkzeug eine Audit-Funktion bereit, die den IT-Mitarbeitern dabei hilft, unterschiedliche Policy Compliance-Anforderungen wie DISA, FISMA, HIPAA, PCI, SOX oder auch STIG zu erfüllen. Dazu verfügt NCM über 169 vorgefertigte Policy Reports für Cisco, Foundry, Juniper und ähnliches. Es besteht aber auch die Option, mit einem Wizard eigene Reports zu generieren die interne Regeln und behördliche Vorgaben abdecken und Reports über die Online-Plattform THWACK auszutauschen. Die Compliance-Regeln werden zudem regelmäßig von SolarWinds und der Community aktualisiert.

Im Test ließen wir zu diesem Zeitpunkt einen Cisco Security Audit Policy-Report laufen. Das geht über "Meine Dashboards / Netzwerkkonfiguration / Compliance", die Auswahl des zu verwendenden Reports (Cisco Security Audit) und die Auswahl des Befehls "Update Selected". Danach läuft der Report durch und zeigt die gefundenen Konfigurationsprobleme (wie zum Beispiel „Disable IP Redirects and IP Unreacheables“), zusammen mit einer Einschätzung ihrer Bedeutung, an. Wenn man nun auf das Icon des jeweiligen Eintrags klickt, erhält man direkt die Möglichkeit, ein Remediation-Skript auf dem betroffenen Gerät laufen zu lassen, das die Konfiguration so anpasst, dass die Compliance gewährleistet wird. Das ist wirklich äußerst einfach und dürfte in vielen Umgebungen eine große Hilfe sein. Die Funktion kann auch in bestimmten Intervallen, beispielsweise täglich, ablaufen und typische Probleme automatisch beheben. Öffnet etwa ein Administrator auf einem Router einen Telnet-Zugang und wurde in dem Compliance-Report festgelegt, dass Telnet im Netz nicht verfügbar sein darf, so stellt die Policy fest, dass es einen Regelverstoß gibt und deaktiviert – falls sie über einen entsprechenden Task verfügt – Telnet und aktiviert bei Bedarf auch gleich SSH. Auf diese Weise bleiben Sicherheitslücken nicht lange bestehen.

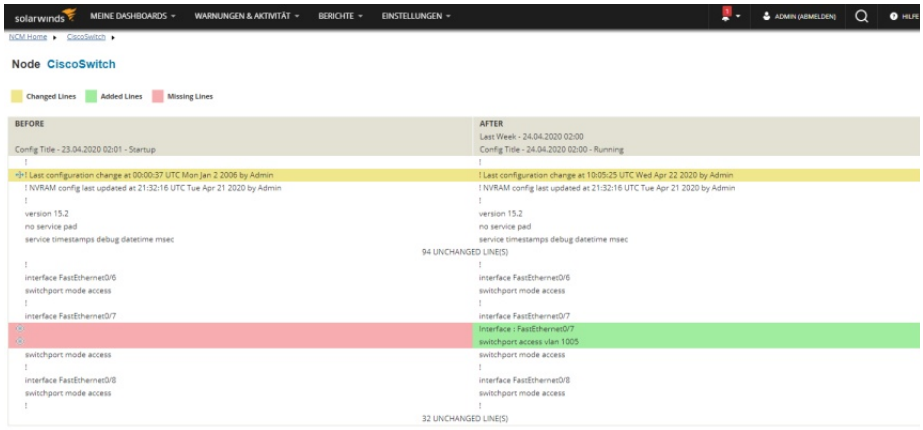
Die Berichtsfunktion

Damit die zuständigen Mitarbeiter immer über den aktuellen Status ihrer Umgebungen im Bilde sind, stellt SolarWinds dem NCM auch eine umfassende Berichtsfunktion an die Seite. Diese bietet 141 vordefinierte Reports zu verschiedenen Aufgabenbereichen wie aktuelle CPU-Lasten, aktive Warnungen oder auch zu den vorhandenen Switch Ports. Diese lassen sich beliebig anpassen, um neue Berichte ergänzen und imsowie exportieren. Außerdem besteht auch die Möglichkeit, die Berichte mit einem Zeitplan automatisch zu erstellen. Um einen Bericht einzusehen, müssen die Anwender nach „Berichte / Alle Berichte“ wechseln, den gewünschten Bericht selektieren (dabei steht ihnen auch eine Suchfunktion zur Verfügung, mit der sich bestimmte Reports schnell auffinden lassen) und dann auf „Bericht anzeigen“ klicken. Danach stellt der NCM den Bericht dar.

Der NCM in größeren Umgebungen und Firmware-Aktualisierungen

Nachdem wir uns nun umfangreich mit dem NCM vertraut ge-

macht hatten, wollten wir einmal sehen, wie sich das Tool in Umgebungen mit mehr als hundert Komponenten verhält. Zu diesem Zweck griffen wir remote auf eine Demo-Umgebung zu, die SolarWinds zu diesem Zweck unter https:// www. solarwinds. com/ network- configuration- manager/ demo-registration zur Verfügung stellt. Dabei stellten wir fest, dass die Arbeit in großen Umgebungen tatsächlich genauso wie in kleinen abläuft. Die Arbeitsschritte sind dieselben, man muss lediglich mehr Zielkomponenten auswählen.



Konfigurationsänderungen hebt das System farblich hervor, um so für Klarheit zu sorgen

Zum Abschluss des Tests aktualisierten wir noch die Firmware unseres Switches von Version 15.2(7)E1 auf Version 15.2(7)E2. Dazu war es zunächst erforderlich, die von Cisco heruntergeladene Update-Datei in ein Share im Netzwerk zu legen, um sie so verfügbar zu machen. Danach wechselten wir im NCM-Interface nach „Meine Dashboards / Netzwerkkonfiguration / Firmware Upgrades“ und hatten dann die Option, einen neuen Upgrade-Vorgang zu definieren. Dafür mussten wir ihm zunächst einen Namen geben und das für unsere Hardware passende Firmware-Upgrade-Template auswählen. Sobald das erledigt war, mussten wir die Update-Datei auswählen. Dazu benötigt man ein Repository. Da wir zu diesem Zeitpunkt noch keines hatten, definierten wir zu diesem Zeitpunkt unser Netzwerk-Share als Repository und ließen den NCM dieses durchsuchen.

Danach konnten wir die zu verwendende Update-Datei auswählen und den zu aktualisierenden Node selektieren. Anschließend sammelte der NCM Informationen von unserem Switch. Diese umfassen den freien Speicherplatz, die Konfiguration und ähnliches. Das System warnt in diesem Zusammenhang auch, wenn zu wenig Speicherplatz auf dem Zieldatenträger verfügbar ist und schlägt Lösungsmöglichkeiten vor, beispielsweise das Sichern und anschließende Entfernen der alten Firmware-Version.

Darüber hinaus lassen sich an dieser Stelle auch noch diverse Optionen festlegen, wie das Speichern der aktuellen Konfiguration im NVRAM vor dem Upgrade, das Verifizieren der Firmware-Image-Integrität und ähnliches. Zum Schluss fragt das System noch, ob es die Ergebnisse per Mail an den Administrator schicken soll, danach lässt sich das Upgrade starten. Im Test ergaben sich während dieses Vorgangs keine Schwierigkeiten.

Ein kleines Problem hatten wir aber während des Testes doch: Wenn der NCM das Repository durchsucht, so findet er standardmäßig nur Firmware-Images, die auf .bin, .tgz, .img oder .imgs enden. Wir hatten im Test unter anderem ein tar-Archiv hochgeladen, das der NCM folgerichtig nicht als Firmware-Upgrade erkannte. Dieses Verhalten lässt sich ändern: Über den Link https:// {Adresse des NCM-Servers}/ Orion/ Admin/ AdvancedConfiguration/ Global.aspx und die anschließende Suche nach dem Begriff „Firmware“ besteht die Möglichkeit, dem Eintrag „Firmware Repository File Extensions“ beliebige zusätzliche Endungen hinzuzufügen. Nachdem wir auf diese Weise die Endung .tar eingetragen hatten, fand die Software auch das Archiv.

Fazit

Zusammenfassend können wir sagen, dass der NCM von SolarWinds eine große Bereicherung für Umgebungen ist, in denen sich Administratoren mit der Verwaltung vieler Netzwerkkomponenten auseinandersetzen müssen. Das Tool vereinfacht das Management der Produkte erheblich, vor allem durch die Templates, die Real-Time-Alerts und die Überwachung der Compliance. Die Lösung schließt nicht nur viele Fehlerquellen aus, sondern spart definitiv auch viel Zeit. Gleichzeitig sorgen die automatischen Reports dafür, dass kein IT-Verantwortlicher die Übersicht verliert. Wir verleihen dem NCM deshalb die Auszeichnung „IT-Testlab Tested and Recommended“.