VMware-Umgebungen mit Runecast analysieren

Im Visier

Jens-Henrik Söldner, Stefan Wacker

Umfangreiche VMware-Umgebungen stellen für den Administrator eine Herausforderung dar. Hier soll Runecast mit automatisierten Analysen potenzieller Fehlerquellen helfen.

Die Komplexität von VMware-Umgebungen hat in den letzten Jahren deutlich zugenommen, da VMware vSphere kontinuierlich erweitert hat und der Hypervisor inzwischen Funktionen zur Netzwerk- und Storage-Virtualisierung umfasst. Zwar bietet VMware selbst kostenpflichtige Managementwerkzeuge wie vRealize Operations oder Log Insight an, allerdings findet man sie aufgrund der Lizenzkosten meist in großen Unternehmen.

Kommt es zu Störungen, können diese Werkzeuge nur bedingt weiterhelfen, da meist Bugs, Inkompatibilitäten, Treiberprobleme oder Fehlkonfigurationen Ausfälle verursachen. Hier kann der Drittanbieter Runecast mit seinem Analyzer helfen, der die zeitaufwendige Analyse und Fehlersuche in vSphere-Umgebungen automatisiert. Runecast lässt sich wie nahezu alle vSphere-Erweiterungen als Appliance im OVF-Format installieren. Danach muss der Administrator das Programm nur noch mit den zu analysierenden Umgebungen verbinden. Hierfür genügt ein Nutzer mit Leserechten auf der virtuellen Infrastruktur.

Anschließend startet der erste Analysevorgang. Die Analyse erfolgt beim Kunden, seine Daten fließen nicht in die Cloud ab. Aus Sicht von vSphere ist Runecast ein einfacher Syslog-Server, den man entweder exklusiv oder zusätzlich zu anderen Syslog-Zielen konfigurieren kann. Darüber hinaus bedient sich Runecast der vSphere-API, um Konfigurationen, Versionsnummern und Hardwareinformationen auszulesen.

Die Informationen über die analysierte Umgebung gleicht der Analyzer mit den gespeicherten Best Practices, Hardening Guides und Knowledge-Base-Artikeln ab. Momentan sind hier vSphere und seit Kurzem vSAN und NSX-V vollständig hinterlegt. Definitionsupdates für die Datenbank kann das System automatisch über das Internet oder manuell über eine ISO-Datei beziehen.

Erster Durchlauf

Nach dem Anmelden landet man auf einem Web-Dashboard, das grob Probleme der Umgebung abbildet. Diese Meldungen sind nach Schweregrad oder Kategorie gegliedert, warnen also vor einem Fehler in der Konfiguration oder der Loganalyse. Die Konfigurationsanalyse vergleicht dabei die Befunde mit Best Practices, Hardening Guide und der Knowledge Base, die Loganalyse jedoch nur mit den KB-Artikeln des Herstellers und von Runecast selbst.

In der Liste der fehlerhaften Konfigurationen findet man dort vieles aus den Hardening Guides und Best-Practice-Dokumenten. Manche Fehler treten erst mit einer bestimmten Kombination von Komponenten und Versionen auf. Runecast erkennt diese durch das Auslesen der Konfiguration von Host und VM und warnt den Administrator. Erweitert man diese Ansicht, kann man Details des zugehörigen KB-Artikels oder Guides nachlesen und sehen, welche Objekte betroffen sind.

Die Software soll durch das Vergleichen der bestehenden Konfiguration mit der Knowledge Base etwaige Fallstricke aufzeigen, bevor sie tatsächlich auftreten. So kann man beispielsweise Fault Tolerance (FT) nicht auf einer VM mit einer virtuellen Intel E1000e aktivieren. Wenn der vSphere-Administrator das nicht weiß, kann es zu längerem Troubleshooting und Neukonfigurieren der VM kommen. Runecast hingegen zeigt bereits, wenn es solche Maschinen findet, dass diese Kombination nicht funktioniert. Jede VMware-Umgebung ist anders. Entsprechend kann man Filter für die Übereinstimmungen mit den Empfehlungen setzen.

Logdateien untersuchen

Damit Runecast Logdateien analysiert, muss man das Senden der Logs von ESXi-Hosts und VMs im Einstellungsmenü konfigurieren. Hier lassen sich außerdem die E-Mail-Benachrichtigung aktivieren und die Filter bearbeiten. Das Programm untersucht zusätzlich zur Konfiguration die Logs, vergleicht also die Meldungen mit Textmustern aus der Knowledge Base und spürt dabei Probleme auf, die so erst mal nicht als Fehlkonfiguration auftreten.

Eine ungünstige Kombination von ESXi, NetQueue und Jumbo Frames beispielsweise zehrt den RAM des Hosts auf. Ohne die Loganalyse würden einem zunächst die Arbeitsspeicherauslastung des Hosts und die Verbindungsabbrüche der Netzwerkkarte auffallen, eine offensichtliche Fehlkonfiguration wäre nicht ersichtlich. Runecast informiert Anwender hier bereits dann, wenn die ersten Symptome in den Logs auftauchen.

Schon länger verfügt Runecast über eine REST-API und kann ebenfalls vSAN und NSX-V analysieren. Seit Version 2.0 kann das System alle einmal erkannten Probleme in der Datenbank speichern. Kunden aus der Finanzindustrie können überprüfen, ob ihre VMware-Umgebung den PCI-DSS-Standard einhält. (fo@ix.de)

Dr. Jens-Henrik Söldner

ist Professor für Wirtschaftsinformatik und IT-Sicherheit an der Hochschule Ansbach sowie Geschäftsführer der Söldner Consult GmbH.

Stefan Wacker

ist als Trainer und Consultant im Bereich Virtualisierung bei der Söldner Consult GmbH in Nürnberg tätig.

© Copyright by Heise Medien
Persönliches PDF für alle Leser der iX aus 30625 Hannover