Automatisiertes Netzwerkmanagement mit Red Hat und F5

Unternehmen sind ständig auf der Suche nach Möglichkeiten, moderne und veraltete Anwendungen zu verbessern. Mit DevOps lassen sich Engpässe beseitigen und Workflows durch Automatisierung beschleunigen. Diese Anwendungen benötigen herkömmliche Services wie Identitäts- und Zugriffsmanagement, Webanwendungssicherheit und TCP-Optimierung, damit Performance und Sicherheit gewährleistet werden können. Darüber hinaus sind Unternehmen durch das Internet verschiedensten Arten von Cyberangriffen ausgesetzt, und der Umfang und die Komplexität dieser Angriffe stellen ein Risiko für sämtliche Systeme dar.

Gemeinsam ermöglichen Red Hat und F5 die Automatisierung, Skalierung und den Schutz von Anwendungs-Workloads in Hybrid Cloud-Umgebungen. Red Hat und F5 bieten gemeinsam Schutz sowohl auf Anwendungs- als auch auf Netzwerkebene.

Automatisierung von Anwendungsinstallation und -Deployment

Die Installation und Verwaltung von Anwendungen auf den einzelnen physischen oder virtuellen Geräten in einem oder mehreren Netzwerken ist oft schwierig, besonders im Hinblick auf die Komplexität einer Hybrid Cloud-Umgebung. Red Hat® Ansible® Automation Platform arbeitet mit F5 zusammen, um Ihnen eine automatisierte Installations- und Bereitstellungsumgebung zu bieten, die die Installation von Anwendungen auf den einzelnen Geräten vereinfacht, die Anzahl der erforderlichen IT-Ressourcen reduziert und die Zuverlässigkeit, Effizienz und Agilität verbessert.

Dazu müssen Sie keine neue Software installieren. Wenn Sie bereits mit F5 arbeiten, können Sie Abläufe mit Ansible Automation Platform durch verschiedene Integrationen mit den F5 BIG-IP-Modulen automatisieren. Sie können F5-Bereitstellungs- und Konfigurationsvorlagen einmalig in einem Ansible Automation Platform Playbook erstellen und diese dann in Ihrem gesamten Unternehmen verwenden.

Mit den F5 Container Ingress Services (CIS) können Sie Ihren Container-Implementierungen auch erweiterte Services für Anwendungen hinzufügen. Dazu gehören Ingress Control HyperText Transfer Protocol (HTTP) Routing, Load Balancing und Application Delivery Performance sowie robuste sicherheitsorientierte Services. Sie können auch Red Hat OpenShift® verwenden, um ein zentrales Portal zur Überwachung von Transaktionen und Sicherheitswarnungen bereitzustellen. Red Hat OpenShift ermöglicht es Ihnen, neue Programmierungen zu validieren, bevor Sie Änderungen vornehmen. So können Sie den Aktualisierungsprozess Ihrer Infrastruktur sicherer gestalten. Sie können diese Änderungen auch ohne Vorausplanung oder Wartungsfenster vornehmen.

Die Fähigkeit festzustellen, wie Anwendungen in Ihren Anwendungen reagieren, ermöglicht Ihnen vorauszuplanen. Sie können komplexe Echtzeitdaten analysieren, um sich plattformübergreifend an veränderte Bedingungen anzupassen, sich vor neuen Bedrohungen zu schützen sowie die von Kunden gewünschten digitalen Erlebnisse zu liefern.

Effiziente Skalierung Ihrer Netzwerkumgebung

Mit Red Hat OpenShift können Sie F5 BIG-IP-Geräte mithilfe von CIS integrieren und Anwendungsservices schneller und mit weniger Aufwand in lokalen und Cloud-Umgebungen bereitstellen. Red Hat OpenShift erleichtert das Entwickeln, Testen und Verwenden von Anwendungen in Ihrer Hybrid- oder Multi-Cloud-Umgebung. Anwendungen können ausgeführt und getestet werden, bevor sie freigegeben und anschließend automatisch zu Ihrer Hybrid- oder Multi-Cloud-Umgebung hinzugefügt werden.

facebook.com/redhatinc
@RedHatDACH
linkedin.com/company/red-hat

Durch die Kombination von Red Hat OpenShift und F5 CIS können Services einmal definiert und dann im gesamten Netzwerk angewendet werden. Die Entwicklerinnen und Entwickler können Anwendungen erstellen und müssen sich dabei keine Gedanken über die Struktur der Kubernetes-Pakete machen, wodurch die Skalierbarkeit in verschiedenen Cloud-Plattformen gewährleistet ist.

Schutz Ihres Netzwerks vor Angriffen von außen

Mit der Ansible Automation Platform und F5 können Sie Sicherheitsprobleme reduzieren – von Fehlern, die auftreten, wenn Anwendungen nicht korrekt zusammenarbeiten, bis hin zu Angriffen von außen, die einen einzelnen Knoten oder Ihr gesamtes System bedrohen. Red Hat OpenShift ermöglicht es Ihnen, die Systeminteraktionen über das Verwaltungsfenster zu überwachen. Dadurch wird die Zeit, in der eine externe Anwendung Zugriff auf Ihr System hat, reduziert.

Durch die Kombination von F5 und Ansible Automation Platform können Sie Ihr gesamtes System auf Sicherheit prüfen und auf Probleme achten, die an verschiedenen Stellen des Systems auftreten können. F5 bietet Schutz vor neuen Bedrohungen, Bot-Erkennung, API-Sicherheit und DDoS-Angriffen (Distributed Denial of Services). Die Ansible Automation Platform kann den Schutz durch Netzwerk-Firewalls, IDS (Intrusion Detection System) und SIEM (Security Information and Detection System) erhöhen.

Die Überwachung Ihres gesamten Systems über ein einziges Fenster gibt Ihnen die Möglichkeit, Probleme zu erkennen, sobald sie auftreten. Anschließend können Sie mithilfe vordefinierter automatischer Workflows Anfragen von anderen Abteilungen weiterleiten, das Problem analysieren und testen und es beheben, indem Sie es ignorieren, den Datenverkehr isolieren oder das Problem beheben und dabei keine anderen Abteilungen benachrichtigen.

Sie können Kubernetes-Objekte mit Red Hat OpenShift überwachen. Erweiterter AWAF-Schutz (Web Application Firewall) und Authentifizierung werden mit verschiedenen Kubernetes-Objekten bereitgestellt und entsprechen den Praktiken der Role-based Access Control (RBAC) von Kubernetes. Wenn BIG-IP Advance WAF oder NGINX App Protect verdächtigen Datenverkehr erkennt, wird eine Warnung mit Details an den ELK-Stack (Elasticsearch, Logstash und Kibana) gesendet, der die Daten indiziert und verarbeitet und dann ein vordefiniertes Ansible Playbook ausführt, um die Sicherheitsrichtlinie durchzusetzen. Sowohl Advanced WAF als auch NGINX App Protect exportieren kontinuierlich detaillierte Daten in Elasticsearch und unterstützen Sie so bei der Überwachung Ihres gesamten Netzwerks und Ihrer Anwendungen. Dieser Ansatz bietet ein ausgewogenes Verhältnis zwischen der Geschwindigkeit neuer Funktionen und der Zuverlässigkeit, auf die sich Ihre Nutzerinnen und Nutzer verlassen können.

Fazit

Mit der zunehmenden Hybridisierung von Umgebungen steigt auch der Bedarf an automatisierter und sicherheitsorientierter Infrastruktur. F5 und Red Hat bieten Ihnen die Tools, mit denen Sie netzwerkübergreifende Aufgaben automatisieren, Installationen und Bereitstellungen auf die für Ihr Unternehmen erforderliche Größe skalieren, sowie Ihre Infrastruktur vor Angriffen schützen können.

Über Red Hat

Red Hat unterstützt Kunden dabei, ihre Umgebungen zu standardisieren, cloudnative Anwendungen zu entwickeln und komplexe Umgebungen mit vielfach ausgezeichnetem Support, Training und Consulting Services zu integrieren, zu automatisieren, zu sichern und zu verwalten.

EUROPA, NAHOST UND AFRIKA (EMEA)
00800 7334 2835
de.redhat.com
europe@redhat.com

TÜRKEI
00800 448820640

ISRAEL
1 809 449548

VAE
8000-4449549

facebook.com/redhatinc
@RedHatDACH
linkedin.com/company/red-hat

de.redhat.com
#F31395_0422