Red Hat과 F5를 통한 네트워크 관리 자동화

기업들은 DevOps를 사용하여 병목 현상을 방지하고 자동화 기술을 통해 워크플로를 가속화하여 최신 및 레거시 애플리케이션을 개선할 방안을 모색하고 있습니다. 이러한 애플리케이션은 성능 및 보안을 유지하기 위해 ID 및 액세스 관리, 웹 애플리케이션 보안, TCP 최적화와 같은 기존 제공 서비스가 필요합니다. 또한 인터넷의 개방성은 조직을 모든 위치에서 사이버 공격에 노출시키고 이러한 공격의 규모와 복잡성은 모든 시스템을 위험에 빠뜨릴 수 있습니다.

Red Hat과 F5는 파트너십을 통해 하이브리드 클라우드 환경에서 애플리케이션 워크로드를 자동화, 확장 및 보호합니다. Red Hat과 F5는 애플리케이션 및 네트워크 수준에서 보호 기능을 제공합니다.

설치 및 배포 작업 자동화

특히 하이브리드 클라우드 환경의 복잡성을 감안할 때, 하나 이상의 네트워크에서 실제 또는 가상 기기에 애플리케이션을 설치 및 관리하는 것은 어려울 수 있습니다. Red Hat® Ansible® 자동화 플랫폼은 F5와 협력하여 자동 설치 및 배포 환경을 제공함으로써 모든 기기에서 애플리케이션 설치를 간소화하고, 필요한 IT 자원량을 줄이고, 신뢰성과 효율성, 민첩성을 향상시킵니다.

플랫폼을 시작하기 위해 새로운 소프트웨어를 설치할 필요가 없습니다. 이미 F5를 사용 중인 경우, F5 BIG-IP 모듈과 일련의 통합을 거친 Ansible 자동화 플랫폼을 사용하여 작업을 자동화할 수 있습니다. Ansible 자동화 플랫폼 플레이북에서 F5 배포 및 구성 템플릿을 한 번 생성한 다음, 귀사의 조직 전반에서 사용할 수 있습니다.

또한 F5 컨테이너 인그레스 서비스(CIS)를 사용하여 컨테이너 배포에 고급 애플리케이션 서비스를 추가할 수 있습니다. 여기에는 인그레스 컨트롤러의 HTTP 라우팅, 로드 밸런싱, 애플리케이션 전송 성능과 더불어 강력한 보안 서비스가 포함됩니다. 아울러, Red Hat OpenShift®를 사용하여 트랜잭션 및 안전 경보를 모니터링하는 단일 창을 제공할 수도 있습니다. Red Hat OpenShift를 사용하면 변경 전에 새로운 프로그래밍을 검증할 수 있으므로, 보다 안전한 인프라 업데이트가 가능합니다. 또한 고급 스케줄링 기능이나 유지관리 기간 없이도 이러한 변경을 수행할 수 있습니다.

그뿐만 아니라, 애플리케이션이 반응하는 방식을 확인할 수 있으므로 미래 예측이 가능합니다. 정교한 실시간 데이터를 분석하여 플랫폼 전반의 변화하는 상황에 적응하고, 진화하는 위협으로부터 방어하며, 고객이 요구하는 디지털 환경을 제공할 수 있습니다.

네트워크 환경을 효율적으로 확장

Red Hat OpenShift를 사용하면 CIS로 F5 BIG-IP 장치를 통합하고, 로컬 및 클라우드 환경에서 애플리케이션 서비스를 더 쉽고 빠르게 배포할 수 있습니다. Red Hat OpenShift는 하이브리드 또는 멀티클라우드 환경에서 애플리케이션의 개발, 테스트 및 적용을 간편하게 만들어줍니다. 애플리케이션을 출시하기 전에 실행 및 테스트한 다음, 귀사의 하이브리드 또는 멀티클라우드 환경에 자동으로 추가할 수 있습니다.

F5 CIS와 결합된 Red Hat OpenShift를 사용하면 서비스를 한 번에 정의하고 네트워크 전체에 적용할 수 있습니다. 개발자는 쿠버네티스 패키지의 구조를 우려할 필요 없이 애플리케이션을 개발할 수 있으며, 클라우드 플랫폼 전반에서 확장이 가능합니다.

외부 공격으로부터 네트워크 보호

Ansible 자동화 플랫폼과 F5는 애플리케이션이 적절하게 호환되지 않는 문제부터 단일 노드 또는 전체 시스템을 위협하는 외부 공격에 이르기까지, 보안 취약점을 최소화하는 데 도움을 줍니다. Red Hat OpenShift를 사용하면 관리 창을 통해 모든 시스템의 상호작용을 모니터링할 수 있으며, 외부 애플리케이션이 귀사의 시스템에 액세스하는 시간을 단축할 수 있습니다.

F5 및 Ansible 자동화 플랫폼을 함께 사용하면 시스템 전체에 신뢰도 높은 보안 검사를 추가할 수 있으므로, 시스템 내에서 발생 가능한 문제를 감시할 수 있게 됩니다. F5는 새로운 위협과 봇 탐지, API 보안 및 분산서비스 거부(DDOS) 공격에 대한 보호 기능을 제공합니다. Ansible 자동화 플랫폼은 네트워크 방화벽과 침입 탐지 시스템(IDS), 보안 정보 및 탐지 시스템(SIEM)을 통해 보호 기능을 추가할 수 있습니다.

단일 창을 통해 시스템 전체를 모니터링하면 문제가 발생하는 즉시 파악할 수 있게 됩니다. 그런 다음 사전 승인된 자동화 워크플로를 사용하여 타 부서의 호출을 라우팅하고, 문제를 분석 및 테스트하고, 문제를 무시하거나 트래픽을 분리하거나 또는 타 부서에 알리지 않은 상태에서 문제를 시정할 수 있습니다.

Red Hat OpenShift를 사용하여 쿠버네티스 객체를 모니터링할 수 있습니다. 고급 웹 애플리케이션 방화벽(AWAF) 보호 및 인증은 다양한 쿠버네티스 객체에 프로비저닝되며, 쿠버네티스 역할 기반 액세스 제어(RBAC) 관행을 준수합니다. BIG-IP Advance WAF 또는 NGINX App Protect가 의심스러운 트래픽을 탐지하는 경우, 세부 사항이 포함된 경보가 Elasticsearch, Logstash 및 Kibana(ELK) 스택에 전송되어 데이터를 인덱싱 및 처리한 다음, 사전 정의된 Ansible Playbook을 실행하여 보안 정책을 실시합니다. Advanced WAF 및 NGINX App Protect는 세부 데이터를 Elasticsearch로 계속 내보내므로, 귀사의 모든 네트워크와 앱을 모니터링할 수 있습니다. 이러한 접근법을 통해 새로운 기능의 속도와 사용자가 의존하는 안정성 간에 균형을 잡을 수 있습니다.

결론

하이브리드 환경이 점점 보편화됨에 따라, 보안 중심의 자동화 인프라에 대한 수요가 높아지고 있습니다. F5 및 Red Hat은 네트워크 전반에서 작업을 자동화하고, 비즈니스에 필요한 크기로 설치 및 배포를 확장하며, 공격으로부터 인프라를 보호하는 데 필요한 도구를 제공합니다.

Red Hat 소개

Red Hat은 고객이 모든 환경을 표준화하고, 클라우드 네이티브 애플리케이션을 개발하며, 복잡한 환경을 자동화, 보호 및 관리할 수 있도록 돕기 위해 수상 이력을 자랑하는 지원, 교육 및 컨설팅 서비스를 제공합니다.

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

북미
1 888 REDHAT1
www.redhat.com

유럽, 중동, 아프리카
00800 7334 2835
europe@redhat.com

아시아 태평양
+65 6490 4200
apac@redhat.com

남미
+54 11 4329 7300
info-latam@redhat.com

redhat.com
#F31395_0422