Red Hat と F5 でネットワーク管理を自動化

企業は、DevOps を使用してボトルネックを解消し、自動化によってワークフローを高速化することで、先進的なアプリケーションとレガシーアプリケーションを強化する方法を模索しています。これらのアプリケーションには、パフォーマンスとセキュリティを確実に維持するために、ID およびアクセス管理、Web アプリケーションのセキュリティ、TCP 最適化など、従来の配信サービスが必要です。さらに、インターネットは本質的にオープンであるため、組織はあらゆる場所からのサイバー攻撃にさらされており、これらの攻撃の規模や周到さによって、いかなるシステムも危険な状態に置かれる可能性があります。

ハイブリッドクラウド環境上でアプリケーションのワークロードを自動化、スケーリング、セキュリティ保護するため、Red Hat と F5 は手を組みました。Red Hat と F5 を組み合わせることで、アプリケーションレベルとネットワークレベルの両方が保護されます。

インストールとデプロイのタスクを自動化

1 つまたは複数のネットワークの全体で物理デバイスや仮想デバイスそれぞれにアプリケーションをインストールして維持するのは、特にハイブリッドクラウド環境では処理が複雑なため、困難になることがあります。Red Hat® Ansible® Automation Platform は F5 と連携して、環境におけるインストールとデプロイを自動化するので、あらゆるデバイスへのアプリケーションのインストールが単純化され、必要な IT リソースが減り、信頼性、効率、アジリティが向上します。

開始するために新しいソフトウェアをインストールする必要はありません。すでに F5 を使用している場合は、F5 BIG-IP モジュールとの一連の統合を通じて、Ansible Automation Platform を使用して運用を自動化できます。Ansible Automation Platform Playbook で F5 のデプロイと構成のテンプレートを一度作成すれば、それらを組織全体で使用できます。

また、F5 Container Ingress Services (CIS) を使用して、高度なアプリケーションサービスをコンテナのデプロイに追加することもできます。これには、イングレスコントロールの HTTP ルーティング、ロードバランシング、アプリケーション提供のパフォーマンスのほか、堅牢なセキュリティ指向のサービスが含まれます。また、Red Hat OpenShift® を使用すると、トランザクションと安全アラートを単一のウィンドウで監視できます。Red Hat OpenShift では、変更を加える前に新しいプログラミングを検証できるため、インフラストラクチャの更新プロセスの安全性が向上します。これらの変更は、高度なスケジューリングやメンテナンス期間なしで行うことができます。

また、組織のアプリケーション内でアプリケーションがどのように反応するかを確認できるため、見通しを立てることが可能になります。洗練されたリアルタイムデータを分析することにより、プラットフォーム全体の状況の変化に適応し、進化する脅威から防御し、顧客が求めるデジタルエクスペリエンスを提供することができます。

ネットワーク環境を効率的にスケーリング

Red Hat OpenShift があれば、CIS を使用して F5 BIG-IP デバイスを統合し、アプリケーションサービスをより短時間かつより少ない労力でローカル環境とクラウド環境にデプロイできます。Red Hat OpenShift を使用すると、ハイブリッド環境やマルチクラウド環境でのアプリケーションの作成、テスト、適用が容易になります。アプリケーションはリリース前に実行してテストした後、ハイブリッド環境またはマルチクラウド環境に自動的に追加できます。

Red Hat OpenShift を F5 CIS と組み合わせて使用すると、サービスを一度定義すれば、ネットワーク全体に適用できます。開発者は、Kubernetes パッケージの構造を気にせずにアプリケーションを作成できるため、複数のクラウド・プラットフォームをまたぐスケーラビリティが実現します。

外部の攻撃からネットワークを保護

Ansible Automation Platform と F5 は、アプリケーションが正しく連携しない場合に発生するエラーや、単一ノードまたはシステム全体を脅かす外部からの攻撃など、セキュリティの問題を軽減するのに役立ちます。Red Hat OpenShift を使用すると、管理ウィンドウからすべてのシステムのやり取りを監視し、外部アプリケーションが組織のシステムにアクセスできる時間を短縮できます。

F5 と Ansible Automation Platform を併せて使用すると、信頼できるセキュリティチェックをシステム全体に追加して、問題がシステム内のどこで発生してもわかるよう監視できます。F5 は、新たに出現する脅威、ボット検出、API セキュリティ、分散型サービス拒否 (DDOS) 攻撃に対する保護を提供します。Ansible Automation Platform は、ネットワーク・ファイアウォール、侵入検知システム (IDS)、セキュリティ情報および検知システム (SIEM) によって保護を強化できます。

単一のウィンドウを使用してシステム全体を監視できるため、問題が発生したらすぐに把握することが可能です。そして、事前承認済みの自動化ワークフローを使用して、他の部門からの呼び出しをルーティングしたり、問題を分析してテストしたりすることができます。また、問題を無視する、トラフィックを分離する、あるいは他の部門に通知せずに問題を修正することによって問題を修正できます。

Red Hat OpenShift を使用すると、Kubernetes オブジェクトを監視できます。高度な Web アプリケーション・ファイアウォール (AWAF) 保護と認証は、さまざまな Kubernetes オブジェクトでプロビジョニングされ、Kubernetes のロールベースのアクセス制御 (RBAC) の手法に準拠しています。BIG-IP Advance WAF または NGINX App Protect が疑わしいトラフィックを検出すると、詳細を含むアラートが Elasticsearch、Logstash、および Kibana (ELK) スタックに送信されます。これにより、データのインデックス作成と処理が行われ、事前に定義済みの Ansible Playbook によりセキュリティポリシーが適用されます。Advanced WAF も NGINX App Protect も詳細なデータを継続的に Elasticsearch にエクスポートするため、すべてのネットワークとアプリケーションを監視することができます。このアプローチにより、新機能のスピードアップとユーザーが求める信頼性を両立できます。

まとめ

環境のハイブリッド化が進むにつれて、自動化されたセキュリティ重視のインフラストラクチャの必要性は高まります。F5 と Red Hat は、ネットワーク全体でタスクを自動化し、インストールとデプロイを組織が必要とする規模にスケーリングし、インフラストラクチャを攻撃から保護するために必要なツールを提供します。

Red Hat について

Red Hat は、受賞歴のあるサポート、トレーニング、コンサルティングサービスをお客様に提供し、複数の環境にわたる標準化、クラウドネイティブ・アプリケーションの開発、複雑な環境の統合、自動化、セキュリティ保護、運用管理を支援します。

アジア太平洋
+65 6490 4200
apac@redhat.com

オーストラリア
1 800 733 428

インド
+91 22 3987 8888

インドネシア
001 803 440 224

日本
03 4590 7472

韓国
080 708 0880

マレーシア
1 800 812 678

ニュージーランド
0800 450 503

シンガポール
800 448 1430

中国
800 810 2100

香港
800 901 222

台湾
0800 666 052

fb.com/RedHatJapan
twitter.com/RedHatJapan
linkedin.com/company/red-hat

jp.redhat.com
#F31395_0422