インフラストラクチャ全体で自動化を保護

「当社のお客様は、Red Hat Ansible Automation Platform を使用して Palo Alto Networks NGFW のデプロイメントとメンテナンスを自動化することで、非常に優れたメリットを享受し、多くの時間を節約しています。たとえば、あるお客様は VM-Series 仮想ファイアウォールのデプロイメントに 3 時間以上かかっていたエンジニアリング時間を 97% 削減し、20 分未満にまで短縮しました。別のお客様は、Ansible を使用して一貫した PAN-OS アップグレードを維持し、[高可用性] HA ペアリングを使用した 75 の NGFW を、数カ月もかけずに 2 時間弱で、時間的余裕がないメンテナンス期間内にアップグレードすることができました」

Rich Campaigna 氏
Palo Alto Networks
プロダクトマネジメント

複雑なインフラストラクチャのセキュリティへの対処

企業のクラウド移行が進む中、チームはより少ないリソースでより多くのことをこなすことが求められており、またネットワークはますます複雑化しています。そのため、特に手作業による処理でさまざまなネットワーク要素を管理し、セキュリティチームがいろいろなツールを使用してコンプライアンスポリシーの構成とデプロイを行っている場合、企業のインフラストラクチャ全体を完全に可視化するのは難しくなります。

その結果、ネットワーク運用チームとセキュリティチームは、ユーザーが世界中のどこからでもアプリケーションやリソースにアクセスできるようにすると同時に、エンタープライズ・アーキテクチャ全体に一貫したセキュリティポリシーを適用して、不正な人物の侵入やデータの流出を防がなければならないというプレッシャーに直面しています。

組織はこれらの課題に対処するために、ネットワーク・インフラストラクチャの管理とメンテナンスを最適化する NetOps 手法の採用を検討しています。しかし、多くの組織で、NetOps を安全に導入するために必要な自動化、オーケストレーション、ソフトウェア・デファインド・ネットワーキングのスキルが欠如しています。

企業全体のセキュリティのためのスピード、スケール、一貫性

Palo Alto Networks® と Red Hat は連携して、ネットワークチームとセキュリティチームが企業のネットワーク・インフラストラクチャを維持し、更新し、保護するための効率的かつ反復可能な NetOps ワークフローを作成し、高度に自動化された方法で重要な環境を保護できるよう支援します。

Palo Alto Networks の PAN-OS® シリーズのファイアウォールと Red Hat® Ansible® Automation Platform を組み合わせることで、ネットワーキングチームは、ネットワークデバイスと環境の変化を管理するための、制御された IaC (Infrastructure-as-Code) アプローチを通じてネットワーク・インフラストラクチャの規模、スピード、セキュリティを向上する NetOps ワークフローを作成できます。

このソリューションは、インフラストラクチャ全体を安全に自動化できるだけでなく、IT チーム間の可視化とコラボレーションを促進します。また、Red Hat と Palo Alto Networks による共同サポートが含まれます。

自動化による効率、応答性、適応性の向上

環境におけるリアルタイムの変化、システムイベント、または外部トリガーに基づいてタスクを自動化する Event-Driven Ansible を使用すると、さらに応答性の高い動的な自動化を実現できます。

PAN-OS 向けの Event-Driven Ansible プラグインによって、Event-Driven Ansible の意思決定機能は、対応が必要な IT 環境の状態に関するインテリジェンスを受信できるようになり、また、Palo Alto Networks 製品のセキュリティ運用が向上します。このプラグインは、リアルタイムのエラーログのストリーミングと自動応答を実現し、ネットワークセキュリティの自己修復を可能にします。

概要：
インフラストラクチャを管理し保護するための、反復可能で一貫性のある運用ワークフローが、自動化によってどのように作成されるかをご覧ください。

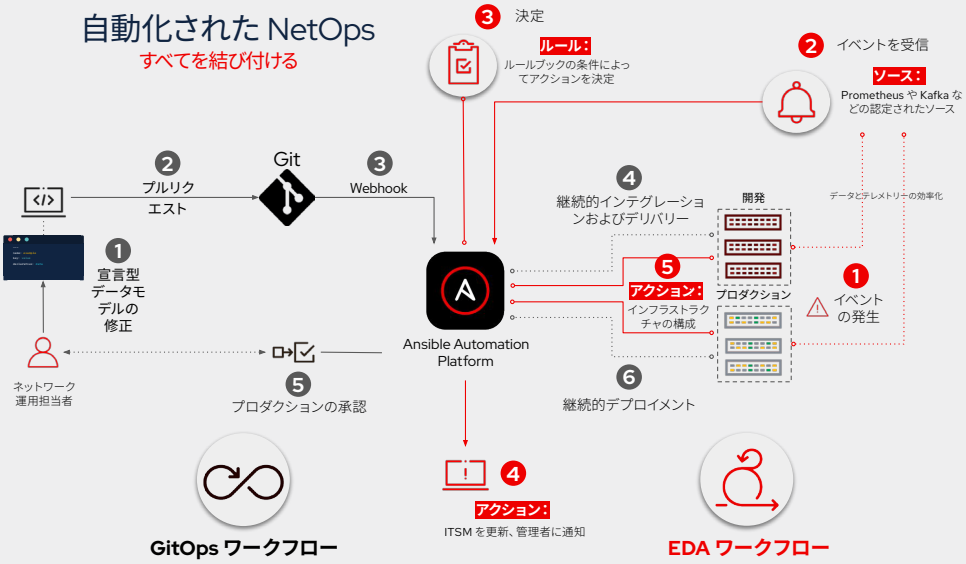

図 1. GitOps 向けの自動化された NetOps の例

Palo Alto Networks の広範な Red Hat Ansible Automation Platform 向け認定コレクションは、Palo Alto Networks の PAN-OS を利用したオファリング (Palo Alto Networks 次世代ファイアウォール (NGFW) を実行するソフトウェア) の自動化を容易にします。この統合により、セキュリティを強化し、運用を最適化し、進化する脅威に適応するための強力なソリューションを得ることができます。

PAN-OS Ansible Content Collection によって、ネットワークチームとセキュリティチームは、単一の自動化プラットフォームを使用して、ネットワークとセキュリティの両方のコンポーネント、構成、ポリシーを定義し管理することができます。

App-ID、Content-ID、Device-ID、User-ID など、PAN-OS に組み込まれている主要テクノロジーを通じて、常に、あらゆる場所のすべてのユーザーおよびデバイスで使用されているアプリケーションを完全に可視化し、制御できます。インライン機械学習 (ML)、アプリケーションおよび脅威シグネチャは、最新のインテリジェンスでファイアウォールを自動的に再プログラムし、許可されたトラフィックに既知および未知の脅威が含まれないようにします。

開発、デプロイ、市場投入までの時間を短縮

PAN-OS Ansible Content Collection をデプロイすると、次のことが可能になります。

- 物理的な次世代ファイアウォールと仮想化された次世代ファイアウォールのデプロイメントを自動化したり、既存の継続的インテグレーションおよび継続的デプロイメント (CI/CD) パイプライン内でデプロイメントを統合したりすることで、時間を節約し、コンプライアンスを強化する。
- 急速な変化に適応し、確信を持ってセキュリティをデプロイする。
- 記録システムにアクセスして、変更管理と監査を目的として構成を検査する。
- 構成を正確に複製し、人為的ミスを排除する。
- 手作業によるプロセスをなくし、各チームが重要な作業に集中できる時間を確保する。

自信を持って NetOps 手法に移行

Palo Alto Networks の PAN-OS シリーズのファイアウォールを Red Hat Ansible Automation Platform と組み合わせることで、インフラストラクチャを自動化し、ネットワーク、セキュリティ、コンプライアンスの運用を安全かつ効率的に管理するために必要なツールが提供され、IT チームがイノベーションに集中できるようになります。以下で詳細をご覧ください。

デモを見る：Red Hat Ansible Automation Platform を使用して Palo Alto Networks 次世代ファイアウォールを自動化

PAN-OS 向けの Ansible の構成方法を確認する

Red Hat と Palo Alto Networks のパートナーシップの詳細

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
#638595_1223