自動化によって特殊作戦部隊を拡張する

スケーラブルな自動化の必要性

手動によるサーバー構成とパッチ適用のプロセスは時間がかかり、ミスが発生しやすいものです。特殊作戦部隊 (SOF) など、グローバルな公共部門の組織は、これらの問題を軽減するためにスケーラブルな自動化ソリューションに移行する必要があります。構成とパッチ適用を自動化すると、手作業によるミスがなくなり、セキュリティが強化されるとともに新機能の提供が迅速化され、スタッフはミッションに特化した高価値の作業に時間を使えます。Red Hat® Ansible® Automation Platform を含む包括的なソリューションは、すべてのハードウェアおよびソフトウェア製品の構成とパッチ適用を自動化し、既存のベンダー固有のツールを単一の統合インタフェースにまとめられます。

手動の防御プロセスのコスト

ネットワークのアップグレードが自動化されている場合でも、サーバー、仮想マシン (VM)、クラウドリソースの構成とパッチ適用は、多くの場合、手作業のプロセスのままです。これらの手動タスクによって以下のことが生じ、戦略的な防衛目標の直接的な妨げとなります。

- 手間のかかる運用：100 台の新しいサーバーのプロビジョニングや、200 台の VM に対する緊急セキュリティパッチの適用といった反復的な手動タスクに対応しなければならないため、マルチドメイン作戦 (MDO) アライアンス (2030 年までにゼロトラスト・サイバーセキュリティ・フレームワークを実現するという NATO の目標) などの重要な戦略的イニシアチブに集中することができません。[1]
- ミッションクリティカルなエラーのリスク：アップグレードやパッチ適用に多段階の複雑な手順があるために、人的ミスのリスクが高まり、重大なセキュリティ脆弱性が生じたり、システム障害に直接つながったりすることがあります。
- 専門知識の誤った配置：管理者が反復的なタスクではなくクリエィティブな作業に専念できるようにすることで、管理者の専門知識をより有効に活用でき、意欲を向上させることができます。

統合されていない自動化を使用するデメリット

機関によっては、いくつかの手動プロセスを自動化済みかもしれませんが、その進捗をさらに加速したいと考えているのではないでしょうか。多くのチームにとっての主要な課題は、ほとんどの自動化ツールが 1 つのベンダーの製品に固有であるということです。VM、物理サーバー、個々のアプリケーション用にそれぞれ用意されているツールを IT チームが学習して管理するのは現実的ではありません。

もう 1 つの障壁は、IT チームが、自分たちのプロセスを自分たちで制御できるという保証を必要としていることです。共有リソースが非常に多いため、各チームは当然のことながら、資産を保護して最適なパフォーマンスを維持するプロセスが、人やシステムによって変更されないようにできるのかという懸念を抱いています。

オープンソースの自動化およびオーケストレーション・ソリューション

ハードウェアおよびソフトウェアの構成とパッチ適用を自動化することで、SOF の IT チームは、一度変更を行えば、ほとんど手間をかけずにすべてまたは一部のデバイスに変更をプッシュすることができます。変更が期待どおりに機能しない場合は、設定を簡単に既知の動作状態に戻せます。

Ansible Automation Platform により、SOF はすべてのハードウェアおよびソフトウェアシステムの構成とパッチ適用を自動化し、高度なワークフローをオーケストレーションすることができます。また、任意のハードウェアまたはソフトウェア製品のコマンドライン・インタフェース (CLI) またはアプリケーション・プログラミング・インタフェース (API) から開始できるあらゆるアクションを自動化できます。Ansible モジュールは、次の 3 種類の方法で取得できます。

1. Red Hat Ecosystem Catalog からモジュールをダウンロードする：Red Hat は 60 を超える独立系ベンダーと連携して、Ansible モジュールの検証と厳選を行っています。これらのモジュールは、Red Hat Ecosystem Catalog で Ansible Content Collections として入手できます。
2. ソフトウェアベンダーおよびハードウェアベンダーからモジュールを購入する：一部のベンダーは、製品を管理するための Ansible モジュールを公開または利用できるようにしています。
3. セルフサービス (DIY)：Red Hat または他のベンダーから特定の製品用のモジュールが提供されない場合は、独自のモジュールを作成できます。

Ansible Automation Platform は、構成とプロセスのアクセス制御に対する IT チームの懸念に対処します。サーバーへのパッチ適用やソフトウェアのアップグレードなどのプロセスを Ansible Automation Platform 内から開始する管理者は、アセット自体にログインすることはありません。その代わり、Ansible Automation Platform が、アセットを所有するチームが定義したアクションを呼び出します。アセットを所有するチームのみがログインできるため、構成ドリフトや特権の昇格などのセキュリティリスクを回避できます。

Red Hat Ansible Automation Platform による SOF ユースケース

ネットワークアクセスの時間制限

ある請負業者がシステムに 24 時間アクセスしなければならない、あるいは機械学習モデルが外部ソースからデータを 48 時間取り込む必要があるとします。どちらのシナリオでも、ファイアウォールポートを開く必要があります。現時点では、管理者は、所定時間の経過後にポートを閉じるよう通知するリマインダーを設定する必要があります。しかし、管理者がこのリマインダーを見なかった場合、または別のタスクで忙しかった場合、ポートは開いたままになり、セキュリティの脆弱性となります。Ansible Automation Platform を使用すると、管理者はジョブを開始したときにジョブが終了するタイミングを指定できます。

一定期間のみ使用するリソースのプロビジョニング

チームは、たとえば特殊作戦部隊 (SOF) の任務をサポートするための機密クラウドリソースのプロビジョニングなど、短期間だけ機能を強化することが必要な場合があります。管理者がミッションの完了後にリソースのスケールダウンを忘れると、必要のないコストが数週間または数カ月にわたって発生する可能性があります。Ansible Automation Platform を使用する場合、管理者はリソースをプロビジョニングする時刻とリソースをリリースする時刻の両方を入力します。

インシデント対応

セキュリティチームは現在、パッチの適用、ポートのクローズ、ユーザーの削除など、デバイスごとに脅威を緩和しています。これらの手作業は手間がかかり、作業の順番が回ってくるまでデバイスは脆弱なままです。Ansible Automation Platform を使用すると、脆弱なすべてのデバイスに一度にアクションを適用できます。

イベント駆動型のアクティビティ

Ansible Automation Platform を他の SOF システムと統合すると、あるシステムでイベントが検出されたら、定義されたアクションを別のシステムで自動的に呼び出すことができます。その例をいくつかご紹介します。

- **VM の要求への対応：**VM の構築にかかる時間は通常 10 分未満です。しかし多くの組織では、リクエストからプロダクションまでが数週間、場合によっては数カ月かかることもあります。あるチームが VM をプロビジョニングし、別のチームが IP アドレスを割り当て、さらに別のチームがオペレーティングシステム (OS) を割り当て、また別のチームがアプリケーションを割り当てます。このようなワークフローでは各ステップで遅延が累積します。Ansible Automation Platform では、VM を要求すると、各チームによってすでに定義されたプロセスがトリガーされ、指定された順序で実行されます。VM のリクエストは 1 日、場合によっては 1 時間で処理できます。
- **Infrastructure as Code (IaC) によるサーバープロビジョニングの自動化：**SOF の開発者は、サーバーのハードウェア、OS、ストレージ、その他のインフラストラクチャ・コンポーネントを手動でプロビジョニングし、管理することができます。しかし、米国国防情報システム局 (DISA) とそのリーダーシップによるガイダンスでは、効率性とセキュリティの向上を目的として IaC への移行を推奨しています。VMware の仮想化ツールや、Amazon Web Services (AWS) や Microsoft Azure などの商用クラウドと統合すると、Ansible Automation Platform は公開されている API を使用してコードを実行し、サーバーを自動的にプロビジョニングします。
- **新しいチームメンバーのオンボーディング：**イベントに応じてアプリケーションのアクティビティを自動化できます。たとえば、オンボーディング・システムが新しいチームメンバーを検出すると、自動化ワークフローがトリガーされ、適切なハードウェアおよびソフトウェアシステム上にアカウントが作成されます。逆に、あるユーザーがチームを離れたことを検出した場合、Ansible Automation Platform は自動的にそのアカウントをアーカイブしたりアクセスを削除したりすることができます。同様に、新しいアプリケーション・エンドポイントを追加すると、ファイアウォールルールの呼び出しや、セキュリティスキャンのトリガー、サービスの利用可能性に関する通知の送信など、自動化されたワークフローをトリガーするように設定することもできます。

SOF で Red Hat Ansible Automation Platform を使用するメリット

Ansible Automation Platform は、以下の理由から効果的で簡単に導入できます。

- **セキュリティ認定を取得済み：**Red Hat Ansible Automation Platform の automation controller に関するセキュリティ技術実装ガイド (STIG) の詳細については、Ansible Content Collections を参照してください。
- **必要なトレーニングまたは再トレーニングが最小限：**Ansible Automation Platform はすでに世界中の SOF チームによって使用されており、導入が単純化されています。
- **ベンダーに依存しない：**Ansible Automation Platform を使用して、アセットの構成とパッチ適用を自動化できます。コア環境から戦術的エッジまでのプラクティスを統合できます。

- **既存のツールを補完：**Ansible Automation Platform により、既存の製品固有の自動化ツールを置き換えるのではなく、すべてのツールを同じインタフェースに統合し、価値を高めることができます。たとえば、IaC に Hashicorp Terraform を使用しているチームは、Ansible Automation Platform から、他の自動化タスクに使用するのと同じインタフェースで Terraform ワークフローを呼び出すことができます。

ルーチンタスクを自動化して SOF のモダナイゼーションを加速する

構成とパッチ適用の自動化は、簡単なアクションで、IT 運用に長期的な効果をもたらします。Red Hat Ansible Automation Platform を使用することで、SOF は同じ人員数でより多くの IT 資産を管理できるようになり、リソースの要求に短時間で対応し、セキュリティポスチャを強化し、スタッフは MDO やゼロトラスト・フレームワークなどの高価値のイニシアチブに取り組む時間を増やすことができます。

さらに詳しく

Red Hat は特殊作戦部隊と提携して、ミッションクリティカルなソリューションを提供します。詳細については Red Hat にお問い合わせください。