Dell CloudIQ Cybersecurity For PowerEdge：自動化のメリット

概要

お客様のインフラストラクチャ チームは、増大するサイバー脅威に対してサーバーを強化するために、さまざまなサーバー設定を選択できます。しかし、セキュリティ構成の設定に関する Dell のベスト プラクティスを確認して使用するにはどうすればよいのでしょうか。また、設定が誤って構成または変更されていることを効率的かつ継続的に確認するにはどうすればよいのでしょうか。その解決策になるのが、CloudIQ for PowerEdge AIOps ソリューションのサイバーセキュリティ機能です。この機能は、導入されている PowerEdge サーバーの構成とセキュリティ関連の構成ポリシーを比較します。CloudIQ は、実際の構成設定と推奨構成設定間の差異を特定すると、管理者に通知し、問題を修正するための修復手順を提示します。

この Direct from Development（DfD）Tech Note では、CloudIQ の自動化されたサイバーセキュリティ ポリシー エンジンを使用することで、手動のコンプライアンス検査と比べてお客様がどれくらい時間を節約できるかについて詳しく説明します。

作成者

Mark Maclean
テクニカル マーケティング エンジニアリング

Kyle Shannon
製品管理

バージョン 1.1：2022 年 7 月

はじめに

今日の常時稼働/常時接続環境では、増大する攻撃の脅威を軽減するために、すべての組織がサイバーセキュリティ戦略を絶えず強化する必要があります。お客様は、Dell CloudIQの組み込み型サイバーセキュリティ機能を使用することで、PowerEdgeサーバーを保護するためのセキュリティ ポリシーを簡単に構築できます。ポリシーは、すぐに使用できるさまざまなテストで構成されます。これらのテストは、チェックボックスをオンにするだけで有効にすることができます。このテストには、Dellのベストプラクティスと NIST（アメリカ国立標準技術研究所）のサイバーセキュリティ フレームワークに基づくインフラストラクチャ セキュリティ設定が含まれています。Dell CloudIQ Cybersecurity for PowerEdgeでは、ポリシーを簡単に作成できるうえ、ポリシー適用を自動化することで、ポリシー適用を単純化、効率化し、予測可能にすることができます。

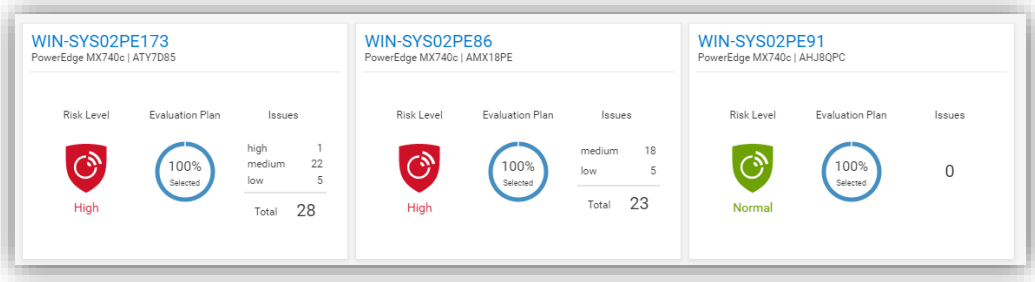


図 1 CloudIQ Cybersecurity のダッシュボード

CloudIQはAIOpsのプロアクティブなモニタリングおよび分析アプリケーションです。ストレージ、データ保護、ネットワーキング、そしてもちろんPowerEdgeサーバーなどのDellインフラストラクチャ ソリューションのシステム正常性に関するインサイトと推奨事項を提供します。CloudIQに組み込まれているサイバーセキュリティ ポリシー エンジンには、簡単に実装可能な30以上のセキュリティ構成ルールがPowerEdge向けに用意されています。CloudIQはクラウドベースであるため、OME CloudIQプラグインを使用することで、複数のデータセンターにまたがって任意の数のOpenManage Enterprise（OME）インスタンスと統合できます。つまりCloudIQは、サーバーの場所を問わずに、OMEが管理する複数のサーバーに同じポリシーを適用できます。これは、CloudIQが提供する機能であり、iDRACまたはOMEレベルで追加の構成を行う必要はありません。ポリシーが設定されると、CloudIQはPowerEdgeセキュリティ構成設定の望ましい状態を「現状」の構成に照らして継続的にチェックします。サーバーがポリシー コンプライアンスに違反していることが判明した場合、そのサーバーが強調表示されます。結果はCloudIQによってスコア付けされ、最も脆弱なサーバーにはリスクレベル「高」が付けられます。個々の問題を、推奨される修復方法とともに確認できます。このセキュリティ構成の推奨修復方法は、iDRAC GUIを使用して、サーバーごとに1対1で実行できます。また、複数のホストがコンプライアンスに違反していることが判明した場合は、OMEを使用して構成更新用のテンプレート ファイルを作成したり、RACADMスクリプトを実行して複数のサーバーのセキュリティ構成を修正したりすることも可能です。

自動化のメリット

このプロセスの自動化による効果の大きさを理解するために、1台、10台、100台*、1,000台*のサーバーを対象として、手動プロセスとの比較テストを実施しました。1,000台*のサーバーを所有しているあるお客様に対してCloudIQ Cybersecurityのアプローチによるテストを実施したところ、次のような結果になりました。

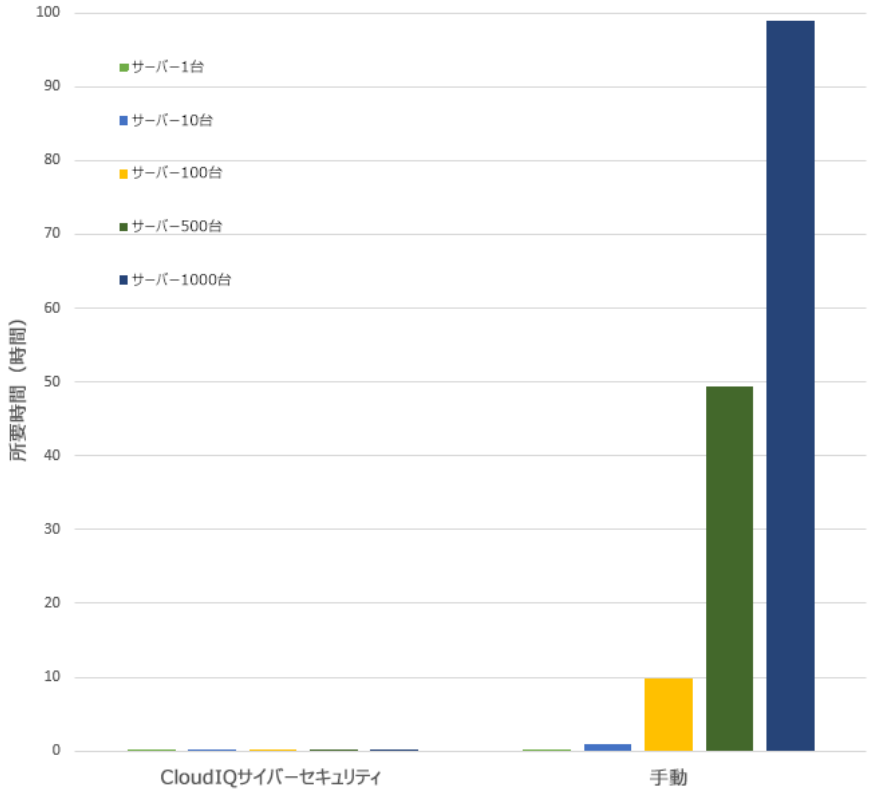
- 3分未満で15のテスト ポリシーを作成して1,000台のサーバーに適用*
- CloudIQのタスクでは手動レビューに比べて実行時間を99%短縮*
- CloudIQではタスク1回の実行時間を98時間短縮*
- CloudIQ Cybersecurityの自動化機能を使用することで、手動に比べて1週間分以上の作業を直ちに節約可能*
- 有効にすると、CloudIQはこれらすべての主要なセキュリティ構成設定を定期的に監視し続ける

*予測される結果は、1台および10台のサーバーの結果の分析に基づきます。お客様の結果は異なる場合があります

ラボ テストでは、iDRAC GUIで15の設定を手動で確認するのにかかった時間が5分56秒だったのに対し、15のアクティブなテスト アイテムで構成されるCloudIQ Cybersecurityポリシーを作成し、ターゲット サーバーを選択するのにかかった時間はわずか2分58秒でした。また、1台、10台、100台、1,000台のサーバーのポリシーを作成するのにかかった時間はすべて同じでした。一方、手動プロセスを使用した場合、チェックにかかる時間はサーバーを追加するごとに5分56秒長くなります。さらに、ポリシーが設定された後も、CloudIQはサーバーの現状の設定がコンプライアンスに準拠しているかどうかを確認し続けます。

結果の概要

タスクの実行時間は短い方が良いことから、次のグラフでは自動プロセスと手動プロセスの違いを強調しています。つまり、自動化によって時間が大幅に節約されることを示しています。



完全な結果データについては、このドキュメントの最後の方にある表 1 をご参照ください。

テストの概要

使いやすさと自動化の効果の両方を実証するために、2つの異なるアプローチ（手動と自動）についてテストを実施しました。CloudIQのサイバーセキュリティ機能を利用するには、OpenManage Enterprise（OME）3.9以降をインストールして、CloudIQプラグイン1.1以降を有効にする必要があります。PowerEdgeサーバーはDell ProSupportの対象であり、ポリシーのターゲット サーバーはすでにOMEによって検出されています。ポリシーを構築するには、CloudIQにサイバーセキュリティ管理者権限が割り当てられている必要があります。テスト用のセキュリティ ポリシーに使用した構成ルールの一部は、iDRACのデフォルト値です。ただし、これらの値はすべて、適切な権限を持つ管理者が個々のiDRACで変更できるため、セキュリティの脆弱性が生じる可能性があります。

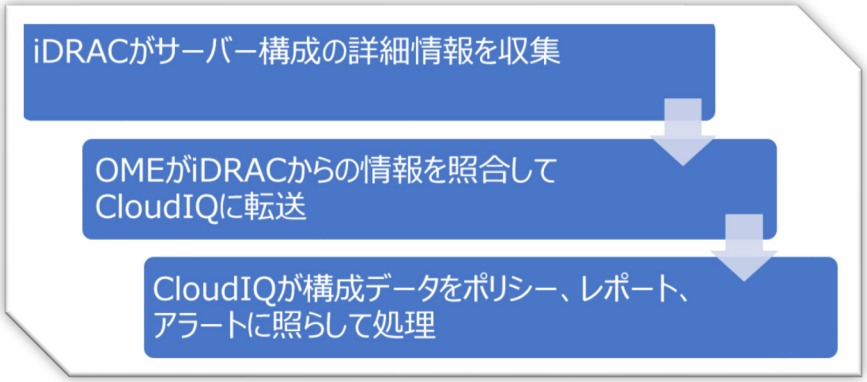


図 2 構成データ フロー

テスト手順

テストのアプローチを正確に比較するために、厳格にテストを実施し、テストを文書化しました。15の共通設定（BIOSとiDRACの構成値の組み合わせ）を選択し、評価版ポリシーで15のテストを有効にしました。テストは、DellのCloudIQ製品を使用して、Dell Austinでテクニカル マーケティングのラボ施設内とオンラインで2022年7月6日に実施しました。

I. USB ポート：無効
II. iDRAC アクティブ NIC：専用
III. System Lockdown：有効
IV. ホストからの iDRAC の構成：無効
V. IPMI over LAN：無効
VI. セキュア ブート：有効
VII. パスワード ポリシー：強
VIII. VNC：無効
IX. SNMP バージョン 3：有効
X. SSH：無効
XI. Syslog：有効
XII. Active Directory 認証：有効
XIII. IP ブロック：有効
XIV. 仮想メディアの暗号化：有効
XV. NTP 時刻同期：有効

CloudIQ の PowerEdge サイバーセキュリティ ポリシーを使用した自動化アプローチの手順

CloudIQ の「サインイン ページ」（https://cloudiq.emc.com）から開始

1. CloudIQ にサインインします
2. 画面の左側にあるメニューから［Cybersecurity］を選択します
3. ［Policy］を選択します
4. ［Templates］タブを選択します
5. ［Add template］を選択します
6. テンプレートに名前を付けます
7. 製品のドロップダウン メニューから［PowerEdge］を選択し、［Next］をクリックします
8. ［Template evaluation plan］で、以下を設定します
9. ［Access Control］で次の項目をオンにします：［IP blocking is enabled］/［SSH is disabled］/［The SNMP configured for V3］/［Active directory authentication is enable］/［VNC disabled］
10. ［Audit and Accountability］で次の項目をオンにします：［NTP time synchronization enabled］/［Remote Syslog enabled］
11. ［Configuration Management］で次の項目をオンにします：［configure iDRAC from Post］/［System lockdown enabled］/［USB ports disabled］
12. ［Identification and Authentication］で次の項目をオンにします：［Password has minimum strength score of strong］
13. ［System and Communications Protection］で次の項目をオンにします：［IPMI over lan disabled］/［virtual media encryption enabled］/［dedicated nic］
14. ［System and information］で次の項目をオンにします：［secure boot enabled］
15. ［Finish］を選択します
16. ［Systems］タブを選択します
17. ホストのリストから必要なホストを選択します（今回のテストでは、1、10、100、1,000 のリストを選択しました）
18. ［Assign］をクリックします。
19. テンプレート リストのドロップダウン メニューから必要なテンプレートを選択します
20. 画面の左側にあるメニューから［System Risk］を選択し、結果を表示します

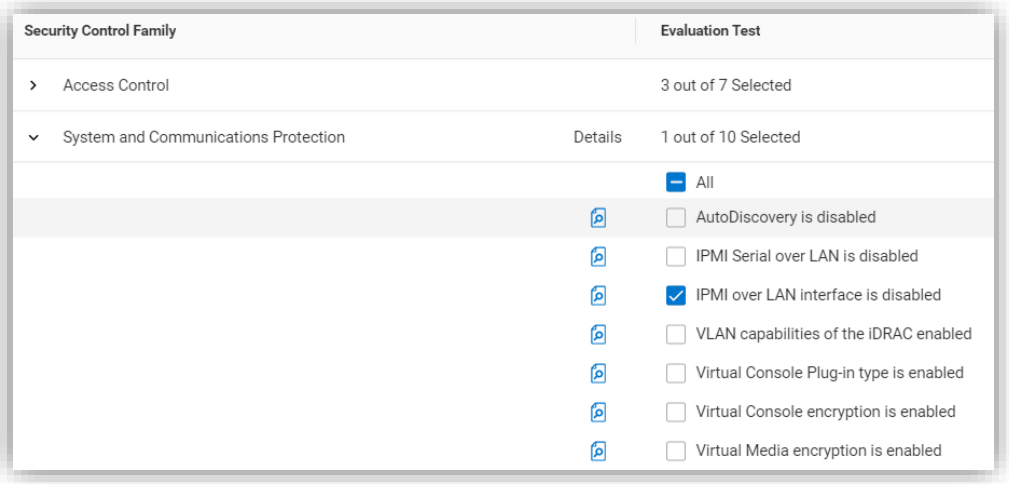


図 3 ポリシーの構築ルールの選択

iDRAC GUI で構成値をチェックする手動アプローチの手順

ブラウザーで iDRAC ログイン画面を表示します。

1. ログインします
2. ［USB］－［Configuration］/［BIOS settings］/［integrated devices］/［user accessible USB ports］：［all ports off］を選択します
3. ［Secure boot］－［Configuration］/［BIOS settings］/［TPM advanced］/［secure boot］：［enabled］を選択します
4. ［VNC］－［Configuration］/［Virtual console］/［VNC server］/［Enable VNC server］：［Disabled］を選択します
5. ［SNMPv3］－［Configuration］/［System setting］/［Alert config］/［SNMP trap］/［SNMP setting］/［SNMP Trap format］：［SNMP v3］を選択します
6. ［Syslog］－［Configuration］/［System settings］/［Alert configuration］/［Remote syslog settings］/［Remote syslog］：［Enabled］を選択します
7. ［Virtual Media encryption］－［Configuration］/［Virtual media］/［Attached media］/［Virtual Media encryption］：［Enabled］を選択します
8. ［Dedicated port］－［iDRAC settings］：［Active］、［NIC interface］：［dedicated］を選択します
9. ［Local iDRAC Config］－［iDRAC settings］/［services］/［local config］/［disable iDRAC local configuration］：［enabled］を選択します
10. ［IPMI］－［iDRAC settings］/［connectivity］/［network］/［IPMI settings］/［Enable IPMI over lan］：［disabled］を選択します
11. ［Password Policy］－［iDRAC settings］/［users］/［global users settings］/［Password setting］/［Policy］/［Score］：［Strong］[1]を選択します
12. ［AD authentication］－［iDRAC settings］/［Users］/［Directory services］/［Microsoft AD］：［Enabled］を選択します
13. ［SSH］－［iDRAC settings］/［services］/［SSH］/［Enabled］：［Disabled］を選択します
14. ［IP blocking］－［iDRAC settings］/［Connectivity］/［Network］/［Advanced networking setting］/［IP blocking］/［Blocking］：［Enabled］を選択します
15. ［NTP time synchronization］－［iDRAC settings］/［settings］/［Time zone］/［NTP server］/［Enable NTP］：［Enabled］を選択します
16. ［Lockdown］－画面右上のパドロック アイコンがロックモードで表示されていることを確認します

Dell PowerEdge R540 BIOS 2.12.2 および iDRAC9 ファームウェア（5.10.00.00）を使用してテストを実施

1. 強力なパスワード ポリシーを手動で適用すると、パスワード ポリシーによって新しいパスワードのコンプライアンスが確保されますが、既存のアカウントでは引き続き脆弱なパスワードが使用されている可能性があり、CloudIQによってパスワードが脆弱なiDRACにフラグが設定されます。

結果

サーバーの数	CloudIQ Cybersecurity ポリシー	手動チェック
1	2 分 58 秒	5 分 56 秒
10	2 分 58 秒	59 分
100	2 分 58 秒	9 時間 53 分*
500	2 分 58 秒	49 時間 26 分*
1,000	2 分 58 秒	98 時間 53 分*

表 *1* - テストの結果

*予測される結果は、1台および10台のサーバーの結果の分析に基づきます。お客様の結果は異なる場合があります

まとめ

今回のテストで、Dell CloudIQ for PowerEdgeサイバーセキュリティ ポリシー エンジンを使用した自動化により、時間効率、再現性、予測可能性、そしてもちろん安心感に関する大きなメリットが得られることが分かりました。また、テスト データでサーバー数を外挿すると、メリットが劇的に増大しました。

参考資料

Dell.com：CloudIQに関するデータ シートおよびデモ ビデオ

ブログ：インテリジェントなクラウドベースのモニタリングによるサーバー サイバーセキュリティの管理

ビデオ：PowerEdgeサーバー用のDell CloudIQ Cybersecurityポリシーの構築および追跡

技術情報ページ：OpenManage Enterprise CloudIQプラグイン

Dellのその他のサイバーセキュリティ関連ソリューション