

Cisco IQ仮想アプライアンス・リリース・ノートv1.2.4

はじめに

Cisco IQTMは、資産の可視性を向上させ、環境全体でよりスマートな洞察を提供するように設計された機能を備えています。さらに、AI AssistantなどのAI機能は、状況に応じた情報に基づいたプロアクティブな意思決定を可能にし、顧客エンゲージメントと成功のためのプロセスを合理化するコンテキスト認識を提供することで、運用成果とCisco IQユーザエクスペリエンスを最適化します。

Cisco IQ On-Prem Air-Gappedは、クラウドに接続できない環境向けに構築されたCisco IQの導入モードです。このアプライアンスは、Cisco IQ Virtual Appliance(VA)と呼ばれる完全独立型の仮想マシン(VM)として提供され、外部ネットワークから完全に分離された状態でお客様の構内で実行されます。Cisco IQ SaaSから取得したソフトウェアアップデートとメンテナンスパッケージは、承認された手動プロセスを通じてVAに転送されます。

規制の厳しい高セキュリティの主権的な環境で業務を行う組織にとって、VAは洞察と制御との間のトレードオフを取り除きます。お客様は、Cisco IQのアセットとアセスメント機能を自社のネットワーク内に導入することで、データの所有権を完全に保持しながら、Cisco IQに期待される見識と推奨事項を得ることができます。エアギャップ導入モードは、分離された環境にCisco IQ SaaSの機能を拡張し、クラウドに接続された企業のスピードと診断インテリジェンスでミッションクリティカルなチームの運用を可能にします。

このドキュメントでは、Cisco IQ VA v1.2.4の新機能、モジュールサポート、および既知の問題について説明します。

主なポイント

資産モジュール

資産モジュールは、シスコ資産の包括的な可視性と管理機能を提供し、Cisco IQの基盤として機能し、組織内のすべてのデバイスの一元化されたリストを提供します。複数の情報源から情報を収集することで、デバイスインベントリの唯一の正しい情報源として機能します。これはダウンロードされたインストーラの一部として使用でき、VAのインストール後に使用可能になります。主な特長は次のとおりです。

資産の重要度の洞察

Asset Criticality Insightsを使用すると、Assetsモジュールでネットワークデバイスの機能の役割とビジネス上の重要性を予測できます。デバイス構成と有効な機能を分析することで、ネットワークに最も大きな影響を与える資産を特定し、セキュリティの修復、ソフトウェアのアップグレード、サポート終了やサポート終了の計画、契約範囲の決定に関して優先順位を付けることができます。

サービス契約

Service Contractsページでは、サポート契約を一元的に監視できます。主な機能は次のとおりです。

- サービス契約の監視：包括的な契約の概要と詳細データにより、更新計画と契約範囲戦略を合理化します。
- 資産固有の洞察：お客様の資産に直接リンクされた明確で実用的なデータにより、脆弱性を迅速に特定して軽減します。

LDOSダッシュボード

サポート終了日(LDOS)ダッシュボードでは、LDOSマイルストーンの一元化されたビューが提供され、ハードウェアまたはソフトウェアがサポート終了に達する前に、資産プランニングと予算予測を改善できるため、運用リスクを大幅に削減できます。

資産のタギング

資産のタグ付けは、カスタムラベルを使用してインベントリを整理、フィルタ、および処理する柔軟な方法を提供します。タグの作成、変更、資産への割り当てを行うことができ、アカウント管理者はタグの一元管理を利用できます。タグを個別の資産に割り当てたり、一括で割り当てたり、タグでインベントリをフィルタリングして、目的の資産をすばやく見つけることができます。

評価モジュール

評価モジュールでは、組織の資産を評価してインベントリを可視化し、セキュリティ、安定性、キャパシティ、コンプライアンス、およびエージングに関連するリスクを予防的に調査して軽減し、ネットワークの安全性を維持するためのフレームワークを提供します。主な特長は次のとおりです。

セキュリティ アドバイザリ

統合型セキュリティアドバイザリを使用すると、潜在的な脅威の一步先に行くことができます。システムは関連する脆弱性をプロアクティブに検知し、重要な更新を確実に通知し、ネットワークを保護するための措置を迅速に講じることができます。

セキュリティの強化

セキュリティの強化では、Cisco OS強化ガイドに照らして資産を継続的に評価することで、ネットワークインフラストラクチャのセキュリティポスチャに対する自動化されたリアルタイムの可視性を提供します。セキュリティ強化の各ルールは、対象資産を通じて評価され、設定の違いを検出します。結果の優先順位は重大度によって決まり、セキュリティギャップの解消、復元力の強化、運用リスクの軽減に役立ちます

コンフィギュレーション

可用性、セキュリティ、またはパフォーマンスに影響を与える可能性があるインフラストラクチャ全体の設定の変更を検出するために、シスコの実績ある専門知識に基づいて、推奨されるベストプラクティスに照らして資産を評価します。システムは、契約対象資産の各ベストプラクティスルールを評価し、設定の一貫性の確保、復元力の強化、運用リスクの軽減に役立てるために、結果を重大度ごとに優先順位を付けます。

Field Notice

Field Noticeでは、ハードウェアとソフトウェアのアップデートに関する通知が適時かつプロアクティブに提供されます。関連するField Noticeを評価ダッシュボード内で直接提示することにより、潜在的な問題が業務に影響を与える前にその問題に対処できます。

AIを活用した機能

Cisco IQ VAはAIを活用した機能を提供し、エアギャップ環境にSaaSグレードのAIインサイトを直接取り入れます。生データを実用的な洞察、推奨事項、ガイド付きアクションに変換することで、Cisco IQを向上させます。AIを利用する機能には、サポートされているGraphics Processing Unit(GPU)を備えたノードが必要です。これらの機能は、CPUのみの導入では有効にできません。機能には、次のものがあります。

- Ask AI Interface:AIを活用したインタラクティブなインサイトに、Assets and Inventoryモジュールから直接アクセスできます。
- LDOS:事前定義されたプロンプトのリストを参照して、サマリーの取得、重要な資産の識別

、LDOS資産の製品ファミリの分析を行うことができます

- 重要な洞察:資産と評価のデータを、実行可能な洞察と推奨事項に変換します。ワークフローに統合され、リアルタイムの洞察とレポートを提供

ソフトウェアライフサイクル管理

VA内のオペレーショナルモジュール、ルール、エンタイトルメント、および専用のAIを活用した機能のソフトウェアライフサイクル（インストールと設定）を管理できます。これらのパッケージは、Cisco IQ(SaaS)から最新バージョンをダウンロードし、System Settings > Package Catalogの順に選択してインストールできます。

Cisco IQコネクタ

Cisco IQ VAには包括的なCisco IQ Connectorが装備されており、直接接続からデバイス、Cisco Catalyst Centerで管理されるデバイスに至る柔軟なテレメトリデータ収集を可能にして、ネットワークの可視性と管理を向上させます。主な特長は次のとおりです。

デバイスの定義

Cisco IQ VAは、デバイスのスコープを定義するための柔軟なオプションを提供します。デバイスを指定するには、CSVファイルをアップロードするか、カンマ区切りリストを手動で入力するか、IP範囲を使用するか、またはCDP(Cisco Discovery Protocol)やLLDP(Link Layer Discovery Protocol)を使用します。このリストは、デバイスを追加または削除するためにいつでも更新でき、デバイスグループを最新の状態に保つことができます。

検出と収集のスケジューリング

Cisco IQ VAは、検出および収集プロセスの独立したスケジューリングを可能にし、特定の日付、時刻、繰り返しパターンをサポートします。これらのタスクは、運用ワークフローに合わせて個別に設定できます。さらに、個々のデバイスに対してオンデマンドの再検出をいつでも実行でき、データ更新サイクルの制御を強化し、トラブルシューティングの応答時間を短縮できます。

サポートされるハイパーバイザ

Cisco IQ VAは、次のハイパーバイザプラットフォームでの導入をサポートしています。導入を開始する前に、インフラストラクチャが特定のハイパーバイザの最小バージョン要件を満たしていることを確認してください。

- VMware ESXi：標準的な仮想化環境をサポート
- Microsoft Hyper-V Server:Windowsベースの仮想化スタックをサポート
- Red Hat Kernel-based VM：オープンソース仮想化環境向けにサポート

非HAマルチノードサポート

Cisco IQ VAは、非高可用性(HA)マルチノードアーキテクチャをサポートし、導入環境の拡張性と柔軟性を高めます。このマルチノードは、管理とワーカーの機能を分離する分散アーキテクチャを提供します。これにより、単一のVAを超えてインフラストラクチャを調整および拡張し、より大規模で複雑なワークロードの要求に対応できます。管理ノードは、クラスタの登録、プラットフォームのインストール、インストール後のモニタリングを行うための主要なインターフェイスとして機能します。

ユーザ マネジメント

次の機能は、ユーザ管理プロセスを簡素化し、システム内のユーザの制御とセキュリティを向上させることを目的としています。

ローカルユーザ管理

ユーザは、個別のアクセス権限を使用して、複数のユーザを安全にオンボーディングおよび管理できます。管理者が作成したローカルユーザは、最初のログイン時にサインアップオプションを使用すると、管理者が設定した電子メールアドレスを使用して安全に自分のパスワードを設定できます。

セルフサービスセキュリティ管理

ローカルセキュリティ設定を個別に管理できるようになり、アカウントのアクセスと回復を制御できるようになりました。セルフサービス機能には、パスワードを忘れた場合にパスワードのリセットする機能や、セキュリティに関する質問を設定する機能が含まれており、外部サポートを必要とせずに、より合理的で安全なユーザエクスペリエンスを実現できます。

Secure SSOのSAML設定

Cisco IQ VAは、Security Assertion Markup Language(SAML)v2.0認証を統合することで、セキュアなシングルサインオン(SSO)機能をサポートします。この統合により、サードパーティのIDプロバイダー(IDP)とのシームレスなIDフェデレーションが可能になり、既存の企業クレデンシャルを使用した認証が可能になります。SAML v2.0を活用することで、組織はセキュリティの強化、ユーザアクセスの合理化、環境全体でのID管理の簡素化を実現できます。同時にアクティブにで

きるIDPは1つだけです。現在、次のIDPがサポートされています。

- オクタIDP
- ADFSのIDP
- エントリIDP

アクティビティログ

すべての運用ログはローカルに保存され、アカウント管理者が表示できるため、ユーザアクティビティを簡単に監視し、透明性を確保できます。

セキュアな標準NTPのサポート

Cisco IQ VAは、セキュアなNetwork Time Protocol(NTP)と標準のNetwork Time Protocol(NTP)の両方をサポートしています。セキュアなNTPでは、Cisco IQ VAと信頼できるNTPサーバ間で認証済みで暗号化された時刻の同期が可能です。一方、標準のNTPでは、暗号化されたNTPデータ交換に対して認証が不要かサポートされていない環境でも同期が可能です。

カスタムSSL証明書のサポート

Cisco IQ VAは、カスタムSSL証明書のインストールと管理をサポートしています。この機能を使用すると、アカウント管理者は、既定の証明書を組織の証明機関(CA)によって発行された証明書に置き換えることができます。カスタム証明書を使用することで、安全で信頼できる通信を確保し、組織の内部セキュリティポリシーへの完全な準拠を維持できます。現在、一度にインストールしてアクティブにできるSSL証明書は1つだけです。

外部syslogサーバのサポート

Cisco IQ VAは外部Syslogサーバとの統合をサポートしているため、アカウント管理者はシステムログを中央集中型のロギングプラットフォームに転送できます。この機能強化により、インフラストラクチャ全体のシステムイベントとセキュリティログの持続的な統合ビューが提供されるため、監視、監査、トラブルシューティングが簡素化されます。最大2台のsyslogサーバを同時に設定できます。

ログインおよびカスタムバナー

Cisco IQ VAでは、設定可能なバナー機能が提供されるようになりました。アカウント管理者は、ログイン画面で必須のシステム通知とセキュリティ警告を設定および表示できます。さらに、ア

カウント管理者は、Cisco IQ VA全体でカスタマイズされたバナーを設定および表示できます。この機能により、重要な情報（通知、免責事項、アラートなど）をCisco IQ VA内のユーザと直接通信できるようになります。

システム管理

Cisco IQ VAの最新のアップデートはSystem Managementタブで表示およびインストールでき、最新の機能、改良、強化された機能に簡単にアクセスできます。Cisco IQ VAは、Cisco IQからプッシュされる自動ソフトウェアアップデートと手動ソフトウェアアップデートの両方をサポートします。手動でアップデートする場合は、System Settings > Package Catalogの順に選択して、Cisco IQ(SaaS)から直接ソフトウェアパッケージをダウンロードできます。

既知の問題

Cisco IQ VAでは、次の問題に積極的に取り組んでいます。

繰り返しスケジュールフィールドにUNIX cron構文が表示される

現在、ネットワークスキャンファイルのアップロードに対して繰り返し入力されるスケジュールには、5つのフィールドを含むUNIXのcron式が必要です（たとえば、「0 2 * * *」）。cron構文に慣れていないユーザは、この入力形式が不明な場合があります。ただし、cronの構文と例に関するより詳細な情報をオンラインで入手できます。

大規模な展開で少数のデバイスでインベントリ収集が断続的に失敗する

現在、10,000台を超えるデバイスの展開では、ディスカバリプロセスが成功しても、少数のデバイスでインベントリ収集を実行できない可能性があります。回避策として、問題のあるデバイスをシステムから取り外し、再度追加します。詳細については、Cisco Technical Assistance Center(TAC)にお問い合わせください。

収集時にエンタイトルメントアップロードステータスが表示されない

現在、権限付与ファイルをアップロードした後、権限付与が正常にロードおよび処理されたことをUIに明示することはできません。権限付与が完全に処理される前にコレクションを開始すると、カバレッジの障害が発生する可能性があります。回避策として、アップロード後1時間以上経過してからコレクションを実行します。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。