Qualys Cloud Agent Windows 5.4

2023 年 11 月付

当該 Cloud Agent リリースの新機能、改善点、プラットフォーム カバレッジの変更、修正についてお知らせします。これらの更新は、エージェント バイナリが対象です。Cloud Agents の管理、同期、タグ付け、レポート機能の新機能と修正に関するプラットフォームの更新は、Cloud Platform と Cloud Suite のリリースノートに記載されています。

新機能

- Qualys Cloud Agent Passive Sensor(QCAPS):この機能により、グローバルなハイブリッド IT 環境全体のすべての管理対象アセットと非管理対象アセットをリアルタイムで可視化できます。

  Qualys Cloud Agent は、監視対象のデバイスのアクティブなプローブを行うことなく、サブネット内のデータを受動的に収集できます。Cloud Agent は、すべてのネットワークトラフィックを監視できます。アセットメタデータは分析のために Qualys Cloud Platform に送信され、管理されていないアセットをオペレーティング システムおよびハードウェア別に分類できます。

  注: この機能は、Windows 8.1 以降でのみサポートされています。

  必須バージョン:Qualys Cloud Platform 3.16.0.0

強化機能

- チャンクダウンロードのサポート — この機能強化により、Cloud Agent はリソース全体を一度に取得するのではなく、リソースまたはアーティファクトをチャンクでダウンロードします。これにより、リソース使用率が最適化され、特に大きなファイルや低速のネットワーク接続を含むシナリオで、ユーザー エクスペリエンスが向上します。

  注: 現在、チャンクのダウンロードは SwCA ファイルと QCAPS ファイルでのみサポートされています。どちらのモジュールも、最初に 1024 KB のチャンク サイズを使用してリソースのダウンロードを試みます。デフォルトでは、チャンクのダウンロードは 3 回再試行され、その後、Cloud Agent は 1 回の操作でリソース全体のダウンロードを試みます。

カスタム評価修復の機能強化 (CAR)

- CAR スクリプト実行後のシステム リブート — ほとんどの修復スクリプトでは、スクリプトの実行にシステムのリブートが必要です。この機能拡張により、手動でリブートしたり、システムリブートに他のツールを使用したりすることなく、CAR ジョブを介してシステムのリブートを開始できます。

  CAR ジョブは、CAR スクリプトを正常に実行した後にシステムをリブートするように設定できます。これは、すべてのスクリプトタイプに適用されます。

  遅延時間、つまりスクリプトの実行後にシステムが再起動されるまでの時間を定義できます。異なる遅延時間を定義して複数のスクリプトを同時に実行すると、システムは最小の遅延時間後に再起動されます。

  必須バージョン: Custom Assessment and Remediation 1.9

パッチ管理の機能強化

- エージェント スキャンの遅延 - この機能強化により、パッチ配布ジョブの進行中にスキャンを延期するオプションが追加されました。これにより、リソースの消費が回避されます。

  必須バージョン: Patch Management 2.6

Qualys Endpoint Detection and Response(EDR)およびエンドポイント保護プラットフォーム (EPP)の機能強化

- EPP ユーザコントロール – EPP マルウェア対策プロファイルを拡張して、指定した URL またはアプリケーションへのアクセスを防止するルールを設定することで、インターネット上のユーザ アクティビティを制御できます。この機能強化により、特定の URL へのアクセスを禁止したり、特定のカテゴリやキーワードを含む URL を禁止または制限したり、指定したアプリケーションをブロックしたりできます。

  必須バージョン:Qualys Endpoint Detection and Response 3.2

- EPP オフラインインストーラ – この機能強化により、サーバではなく特定の場所から EPP インストーラをダウンロードするように Cloud Agent を設定できます。EPP インストーラは、ローカルの HTTP サーバまたはローカルシステム上の任意の場所でホストできます。これにより、Qualys EPP の迅速なインストールが可能になり、Qualys EPP インストールをダウンロードするための時間と帯域幅の要件が削減されます。

  クイックインストールにより、Qualys EPP をインストールする前に他のセキュリティソフトウェアをアンインストールする必要があるため、システムの脆弱性の期間が短縮されます。

  必須バージョン:Qualys Endpoint Detection and Response 3.1

- ファイルレス マルウェア検出 – この機能強化を使用すると、実行前の段階でコマンドライン引数を使用して実行するファイルレス マルウェアを検出するように Qualys EPP を設定できます。

  必須バージョン:Qualys Endpoint Detection and Response 2.7

- 他のセキュリティソフトウェアの OPSWAT ベースのアンインストール – Cloud Agent は、OPSWAT ベースの検出およびアンインストール機能を利用して、Qualys EPP をインストールする前に他のセキュリティアプリケーションをアンインストールします。これらのアプリケーションは、Qualys EPP と共存できず、相互運用性を引き起こす可能性があるため、削除する必要があります。

  必須バージョン: Endpoint Detection and Response 2.7

- EPP プロキシ サーバのサポート – この機能強化により、Qualys EPP は Cloud Agent for Windows と同じプロキシ設定を使用できます。これにより、プロキシの障害が原因で EPP マルウェア対策更新プログラムがダウンロードされないシナリオを防ぐことができます。

  たとえば、プロキシ経由の接続が失敗したときに、Cloud Agent が Qualys Cloud Platform への直接接続を試みた場合などです。この場合、Qualys EPP は直接接続を使用して Qualys Cloud Platform に接続します。

動作の変更点

このリリースでは、動作の変更はありません。

プラットフォーム カバレッジ サポート (オペレーティング システム)

Windows 10 IoT LTSC 2019 および 2021 のサポートが追加されました。

修正された不具合

以下はこのリリースで重要な問題として修正されています。

CRM-113418	ネットワーク共有の監視中に除外されたユーザー名の FIM イベントが記録される問題を修正しました。
CRM-111775	プロキシ経由の接続がエラーコード 12175 で失敗したときに、Cloud Agent が Qualys Cloud Platform への直接接続を試みない問題を修正しました。

既知の制限事項と回避策

このリリースには、報告された問題や注目すべき問題はありません。