Cloud Agent

操作ガイド

2018 年 3 月 2 日

無断複写・転載を禁じます。2015-2018 年 クォリスジャパン株式会社

Qualys および Qualys のロゴは、Qualys, Inc. の登録商標です。その他のすべての商標は各所有者に帰属します。

クォリス ジャパン株式会社
〒 100-6208
東京都千代田区丸の内 1-11-1
パシフィックセンチュリープレイス 8 階
03-6860-8296

目次

本書について 4
Qualys について 4
Qualys サポート 4

はじめに 5
概要 5
知っておく必要があること 5
利用できる Cloud Agent プラットフォームのマトリックス 8
Cloud Agent プラットフォームの Windows に必要なホットフィックス 12
簡単にエージェントをインストール 13
AWS でのエージェントのインストール 16
アセットデータをクラウドに同期！ 16
クラウドの継続スキャン 17

エージェントの管理 18
エージェントの概要 18
エージェントのステータスについて 19
アクティブ化ジョブの進行状況の表示 20
現在のアセットの詳細を簡単に表示 22
エージェントへの一括アクション 23
設定の変更 23
エージェントホストのタグ付け 24
エージェントファイルを検索していますか？ 25

Qualys プラットフォームアプリケーションの使用 26
Vulnerability Management 26
Policy Compliance 29
Continuous Monitoring 30

本書について

当社の画期的な新製品 Qualys クラウドエージェントプラットフォームに関心をお寄せいただきありがとうございます。この新しいプラットフォームは Qualys クラウドプラットフォームを拡張したもので、軽量エージェントを使用してグローバルな IT インフラおよびアプリケーションを継続的に評価します。お客様は IT アセットにエージェントをインストールするだけです。本書はこのプラットフォームをすぐに使い始められるようにするためのガイドです！

Qualys について

Qualys, Inc.（NASDAQ: QLYS）は、セキュリティおよびコンプライアンスを目的とするクラウドベースソリューションのパイオニアであり、リーディングカンパニーです。Qualys の製品は、「Forbes Global 100」および「Fortune 100」の大多数を占める、世界 100 か国の 9,300 を超える顧客に採用されています。Qualys クラウドプラットフォームおよび統合されたアプリケーションスイートは、重要なセキュリティインテリジェンスをオンデマンドで提供し、IT システムと Web アプリケーションの監査、コンプライアンス、および保護の全範囲を自動化することにより、ビジネスにおけるセキュリティ業務の簡略化とコンプライアンスのコスト削減を支援します。1999 年の創立以来、Qualys は、Accenture、BT、Cognizant Technology Solutions、富士通、HCL Comnet、HPE、InfoSys、NTT、Optiv、SecureWorks、Tata Communications、Verizon、Wipro などのマネージドサービスプロバイダやコンサルティング企業との戦略的パートナーシップを構築してきました。Qualys は、CSA（Cloud Security Alliance）の創立メンバーでもあります。詳細情報は、www.qualys.com をご覧ください。

Qualys サポート

Qualys は綿密なサポートを提供します。不明な点には、オンラインドキュメント、電話サポート、および E メールによる直接サポートを通じて、可能な限り迅速にお答えします。弊社は 24 時間年中無休でサポートを提供します。サポート情報については、www.qualys.com/support/ をご覧ください。

はじめに

Qualys クラウドエージェントがあれば、クラウド経由でネットワークセキュリティの更新を継続的に取得することができます。ホストの変更は検出されると同時に評価され、新しいセキュリティ上の脅威について即時に通知されます。お客様はホストに軽量エージェントをインストールするだけです。この操作をすばやく行うための手順を説明します！

概要

ご使用の　IT　アセットに数分で**軽量エージェントをインストール**します。稼働中のシステムにも、動的クラウド環境にも、モバイルエンドポイントにもインストールできます。エージェントはクラウドエージェントプラットフォームによって一元管理され、自動更新します（再起動は不要です）。

クラウドでのスキャン エージェントがインストールされると、すぐにアセットデータとクラウドエージェントプラットフォームの同期を開始します。エージェントはメタデータの収集を続け、クラウドエージェントプラットフォームに送信し、プラットフォームではこのデータの完全評価が即時実行されます。最も負荷がかかる作業はクラウドで行われるため、エージェントに必要なフットプリントとターゲットシステムでの処理は最小限に抑えられます。

常にネットワークセキュリティの最新状態を把握 クラウドのスキャンは、従来の Qualys スキャナによるスキャンと同じシグニチャ（脆弱性、コンプライアンス、データポイント数）を使用します。新しいセキュリティ上の脅威に関する情報は、Qualys クラウドプラットフォームアプリケーション（Vulnerability Management（VM）、Policy Compliance（PC）、Continuous Monitoring（CM）、AssetView（AV）、その他各種）を使用して即時把握できます。

知っておく必要があること

ネットワークにあるホストにエージェントをインストールする前に確認しておく情報がいくつかあります。

Qualys Cloud Agent（CA）についての説明を見る

ビデオチュートリアル

クラウドエージェントプラットフォームの概要（2 分 10 秒）

操作チュートリアル（4 分 58 秒）

Cloud Agent の要件

- サポート対象のシステム : Windows、Linux/Unix（.rpm）、Linux（.deb）、Apple Mac OSX（.pkg）

利用できる Cloud Agent プラットフォームのマトリックス

- ホストから HTTPS ポート 443 経由で Qualys クラウドプラットフォーム（または Qualys プライベートクラウドプラットフォーム）にアクセスできる必要があります。ホストからアクセスする必要のある URL を表示するには、「ヘルプ」→「一般情報」を選択します。

- Windows エージェントをインストールするには、ホストに対するローカル管理者権限が必要です。プロキシ設定がサポートされています。

- Linux エージェント、Unix エージェント、Mac エージェントをインストールするには、ルート権限、Sudo によってルート権限を委譲された非ルート権限、または十分な特権のある非ルート権限が必要です（VM スキャンのみ）。プロキシ設定がサポートされています。

エージェントのインストール手順

- アクティブ化キーを作成します。これにより、エージェントをグループ化してアカウントにバインディングできます。

- エージェントインストーラをダウンロードして、ローカルマシンに保存します。

- 各ホストでコマンドプロンプトから昇格した権限でインストーラを実行するか、またはグループポリシーあるいはシステム管理ツールを使用します。

- サブスクリプションのモジュールに対してエージェントをアクティブ化します（VM または PC）。ライセンスはアクティブ化された各エージェントに対して割り当てられます。

クイックスタートガイドを始める

クイックスタートガイドをご確認ください（ユーザ名メニューからクイックスタートガイドのオプションを選択します）。画面の左側には、手順に沿った説明が、操作を行うために適切な場所へのリンクとともに表示されます。右側には、ビデオチュートリアルへのリンクが表示されます。

ヒント - 「**Cloud Agent の概要**」をクリックすると、要件やプロキシ対応などについての有益な情報を入手できます。

トレーニングをお探しの場合は、以下のオプションをご覧ください。

無料トレーニング

CA 無料自学コース

CA ビデオライブラリ

利用できる Cloud Agent プラットフォームのマトリックス

Windows | Linux | Unix | Apple Mac

Windows

最新のリリース : 1.6.3.8、2.0.2.192*

サポートが終了したバージョン : 1.3.0.18、1.4.0.x

*FIM や IOC を有効にしている顧客に対する最新のリリース

サポートされているプラットフォーム				サポートされている Qualys モジュール/エージェントのバージョン				
ベンダ	オペレーティングシステム	アーキテクチャ	インストーラ	インベントリ	VM	PC	FIM	IOC
Microsoft	Windows XP SP 3+	x86_64（1.6 の場合）x86_32（旧バージョンの場合）	(.exe)	1.4.5.232-1.6.2.19、2.0.2.192	1.4.5.232-1.6.2.19、2.0.2.192	1.4.5.232-1.6.2.19、2.0.2.192	2.0.2.192	2.0.2.192
Microsoft	Windows Vista	x86_64（1.6 の場合）x86_32（旧バージョンの場合）	(.exe)	1.4.5.232-1.6.2.19、2.0.2.192	1.4.5.232-1.6.2.19、2.0.2.192	1.4.5.232-1.6.2.19、2.0.2.192	2.0.2.192	2.0.2.192
Microsoft	Windows 7	x86_64（1.6 の場合）x86_32（旧バージョンの場合）	(.exe)	1.4.5.232-1.6.2.19、2.0.2.192	1.4.5.232-1.6.2.19、2.0.2.192	1.4.5.232-1.6.2.19、2.0.2.192	2.0.2.192	2.0.2.192
Microsoft	Windows 8/8.1	x86_64（1.6 の場合）x86_32（旧バージョンの場合）	(.exe)	1.4.5.232-1.6.2.19、2.0.2.192	1.4.5.232-1.6.2.19、2.0.2.192	1.4.5.232-1.6.2.19、2.0.2.192	2.0.2.192	2.0.2.192
Microsoft	Windows 10（1511、1607、1703、1709）	x86_64（1.6 の場合）x86_32（旧バージョンの場合）	(.exe)	1.4.5.232-1.6.2.19、2.0.2.192	1.4.5.232-1.6.2.19、2.0.2.192	1.4.5.232-1.6.2.19、2.0.2.192	2.0.2.192	2.0.2.192
Microsoft	Windows Server2003SP2 以降	x86_64（1.6 の場合）x86_32（旧バージョンの場合）	(.exe)	1.4.5.232-1.6.2.19、2.0.2.192	1.4.5.232-1.6.2.19、2.0.2.192	1.4.5.232-1.6.2.19、2.0.2.192	2.0.2.192	2.0.2.192
Microsoft	Windows Server 2008/R2*	x86_64（1.6 の場合）x86_32（旧バージョンの場合）	(.exe)	1.4.5.232-1.6.2.19、2.0.2.192	1.4.5.232-1.6.2.19、2.0.2.192	1.4.5.232-1.6.2.19、2.0.2.192	2.0.2.192	2.0.2.192

サポートされているプラットフォーム				サポートされている Qualys モジュール/エージェントのバージョン				
ベンダ	オペレーティングシステム	アーキテクチャ	インストーラ	インベントリ	VM	PC	FIM	IOC
Microsoft	Windows Server 2012/R2*	x86_64（1.6 の場合） x86_32（旧バージョンの場合）	(.exe)	1.4.5.232-1.6.2.19、2.0.2.192	1.4.5.232-1.6.2.19、2.0.2.192	1.4.5.232-1.6.2.19、2.0.2.192	2.0.2.192	2.0.2.192
Microsoft	Windows Server 2016*	x86_64（1.6 の場合） x86_32（旧バージョンの場合）	(.exe)	1.5.6.46 1.6.2.19、2.0.2.192	1.5.6.46 1.6.2.19、2.0.2.192	1.5.6.46 1.6.2.19、2.0.2.192	2.0.2.192	2.0.2.192

* すべてのエディションと Server Core を含む

重要情報 : Cryptography Next Generation（CNG）Suite B アルゴリズム（SHA2 を含む）に対応していない Windows XP および Windows Server 2003 は、このマトリックスのオペレーティングシステムには含まれていません。Qualys の認証では、SHA2-512 を使用しており、そのような認証に対して実行する検証では、プラットフォームがアルゴリズムに対応していないことが原因となり、インストールされている証明書を検証したり、証明書をインストールしたりすることはできません。ホットフィックスをインストールし、システムに必要な SHA2-256/318/512 を追加して対応できるようにする必要があります。

必要なホットフィックスについてはこちらをクリック

Linux

最新のリリース : 1.6.0.61、2.0.2.79*

サポートが終了したバージョン : 1.3.3.23、1.3.1.16

*FIM を有効にしている顧客に対する最新のリリース

サポートされているプラットフォーム				サポートされている Qualys モジュール/エージェントのバージョン				
ベンダ	オペレーティングシステム	アーキテクチャ	インストーラ	インベントリ	VM	PC	FIM	IOC
Red Hat	Red Hat Enterprise Linux 5.4x	x86_64	(rpm)	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	使用不可	使用不可
Red Hat	Red Hat Enterprise Linux 6	x86_64	(rpm)	1.5.0.61-1.6.0.61、2.0.2.79	1.5.0.61-1.6.0.61、2.0.2.79	1.5.0.61-1.6.0.61、2.0.2.79	2.0.2.79 (RHEL 6.5+)	使用不可
Red Hat	Red Hat Enterprise Linux 7	x86_64	(rpm)	1.5.0.61-1.6.0.61、2.0.2.79	1.5.0.61-1.6.0.61、2.0.2.79	1.5.0.61-1.6.0.61、2.0.2.79	2.0.2.79	使用不可
Red Hat	CentOS5.4 以降	x86_64	(rpm)	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	使用不可	使用不可
Red Hat	CentOS 6	x86_64	(rpm)	1.5.0.61-1.6.0.61、2.0.2.79	1.5.0.61-1.6.0.61、2.0.2.79	1.5.0.61-1.6.0.61、2.0.2.79	2.0.2.79 (CentOS 6.5+)	使用不可
Red Hat	CentOS 7	x86_64	(rpm)	1.5.0.61-1.6.0.61、2.0.2.79	1.5.0.61-1.6.0.61、2.0.2.79	1.5.0.61-1.6.0.61、2.0.2.79	2.0.2.79	使用不可

	サポートされているプラットフォーム			サポートされている Qualys モジュール/エージェントのバージョン				
ベンダ	オペレーティングシステム	アーキテクチャ	インストーラ	インベントリ	VM	PC	FIM	IOC
Red Hat	Fedora 22、23、24	x86_64	(rpm)	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	使用不可	使用不可	使用不可
SUSE	SUSE Linux Enterprise 11、12	x86_64	(rpm)	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	使用不可	使用不可
SUSE	OpenSUSE 12	x86_64	(rpm)	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	使用不可	使用不可	使用不可
SUSE	OpenSUSE 13	x86_64	(rpm)	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	使用不可	使用不可
SUSE	OpenSUSE Leap 42.1	x86_64	(rpm)	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	使用不可	使用不可	使用不可
Amazon	Amazon Linux 2015.09	x86_64	(rpm)	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	使用不可	使用不可	使用不可
Amazon	Amazon Linux 2016.09	x86_64	(rpm)	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	使用不可	使用不可
Amazon	Amazon Linux 2017.03	x86_64	(rpm)	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	使用不可	使用不可
Amazon	Amazon Linux 2017.09	x86_64	(rpm)	1.6.0.61	1.6.0.61	1.6.0.61	使用不可	使用不可
Oracle	Oracle Enterprise Linux 5.11	x86_64	(rpm)	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	使用不可	使用不可
Oracle	Oracle Enterprise Linux 6、7	x86_64	(rpm)	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61,	使用不可	使用不可
Debian	Debian 7.x、8.x	x86_64	(deb)	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	使用不可	使用不可
Ubuntu	Ubuntu 12.x	x86_64	(deb)	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	使用不可	使用不可
Ubuntu	Ubuntu 14.x	x86_64	(deb)	1.5.0.61-1.6.0.61、2.0.2.79	1.5.0.61-1.6.0.61、2.0.2.79	1.5.0.61-1.6.0.61、2.0.2.79	2.0.2.79	使用不可
Ubuntu	Ubuntu 15.x	x86_64	(deb)	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	使用不可	使用不可	使用不可
Ubuntu	Ubuntu 16.04	x86_64	(deb)	1.5.0.61-1.6.0.61、2.0.2.79	1.5.0.61-1.6.0.61、2.0.2.79	使用不可	2.0.2.79	使用不可

IBM AIX

最新のリリース : 1.6.2

	サポートされているプラットフォーム			サポートされている Qualys モジュール/エージェントのバージョン				
ベンダ	オペレーティングシステム	アーキテクチャ	インストーラ	インベントリ	VM	PC	FIM	IOC
IBM	AIX 7.1 TL2、TL3、TL4 AIX 7.2 TL1 （Standardおよび Enterprise Edition）	POWER 64 ビット版	(rpm)	1.6.2	1.6.2	1.6.2	使用不可	使用不可
IBM	AIX 6.1 TL0-9 （Standardおよび Enterprise Edition）	POWER 64 ビット版	(rpm)	1.6.2	1.6.2	1.6.2	使用不可	使用不可

Apple Mac

最新の GA リリース : 1.6.0.61

	サポートされているプラットフォーム			サポートされている Qualys モジュール/エージェントのバージョン				
ベンダ	オペレーティングシステム	アーキテクチャ	インストーラ	インベントリ	VM	PC	FIM	IOC
Apple	OS X Yosemite （10.10）	x86_64	(rpm)	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	使用不可	使用不可
Apple	OS X El Capitan （10.11）	x86_64	(rpm)	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	使用不可	使用不可
Apple	macOS Sierra （10.12）*	x86_64	(rpm)	1.6.0.61	1.6.0.61	1.6.0.61	使用不可	使用不可
Apple	macOS High Sierra（10.13）	x86_64	(rpm)	1.6.0.61	1.6.0.61	使用不可	使用不可	使用不可

* El Capitan（10.11）から Sierra（10.12）にアップグレードした場合、エージェントで使用する必要なディレクトリが削除され、エージェントが起動しなくなります。以下のコマンドを使用して、ディレクトリを修復してください。

1）mkdir /var/log/qualys

2）chmod 640 /var/log/qualys

3）root 以外の場合 : chown non-root.non-root-group /var/log/qualys

4）/Applications/QualysCloudAgent.app/Contents/MacOS/qagent_restart.sh

Cloud Agent プラットフォームの Windows に必要なホットフィックス

次のホットフィックスは、Windows エージェントの正常なインストールに必要です。

Windows XP SP3 x86 の SHA2 証明書ホットフィックス

KB 記事番号 : 968730

言語 : 英語

プラットフォーム : i386

場所 :

http://hotfixv4.microsoft.com/Windows%20XP/sp4/Fix251294/2600/free/375554_ENU_i386_zip.exe

Windows XP SP3 x86 の SHA2 証明書ホットフィックス

KB 記事番号 : 968730

言語 : 英語

プラットフォーム : i386

場所 :

http://hotfixv4.microsoft.com/Windows%20Server%202003/sp3/Fix262679/3790/free/375510_ENU_i386_zip.exe

Windows XP x64 および Windows Server 2003 x64 SP3 の SHA2 証明書ホットフィック

KB 記事番号 : 968730

言語 : 英語

プラットフォーム : x64

場所 :

http://hotfixv4.microsoft.com/Windows%20Server%202003/sp3/Fix262679/3790/free/375531_ENU_x64_zip.exe

KB 記事番号 : 968730

言語 : 英語

プラットフォーム : i386

場所 :

http://hotfixv4.microsoft.com/Windows%20Server%202003/sp3/Fix262679/3790/free/375510_ENU_i386_zip.exe

Microsoft KB 記事（この修正に必要なその他のホットパッチ）：

http://support2.microsoft.com/hotfix/KBHotfix.aspx?kbnum=968730&kbln=en-US

簡単にエージェントをインストール

エージェントはほんの数分でインストールできます。ウィザードに従えばすばやく設定できます！

手順を説明

ウィザードを開始 「エージェント管理」を選択し、「アクティブ化キーを管理」を選択します（または「アクティブ化キー」タブに移動します）。

「新規キー」を選択して新規アクティブ化キーを作成します。アクティブ化キーを使用してエージェントをインストールします。

アクティブ化キーにより、エージェントをグループ化してアカウントにバインディングできます。

例えば、さまざまなビジネス機能とユーザにそれぞれ異なるキーを作成できます。

すでにキーがある場合は、リストからキーを選択し、「クイックアクション」メニューから「エージェントをインストール」を選択します。

新規アクティブ化キーを生成 「生成」ボタンをクリックします。

後で簡単に分るように、キーに意味のある名前を付けます。

タグを追加するのは、エージェントの管理が容易になるためです。タグは、エージェントホストに関連付けられます。

キーにはデフォルトで制限はありません。任意の数のエージェントをいつでもインストールできます。

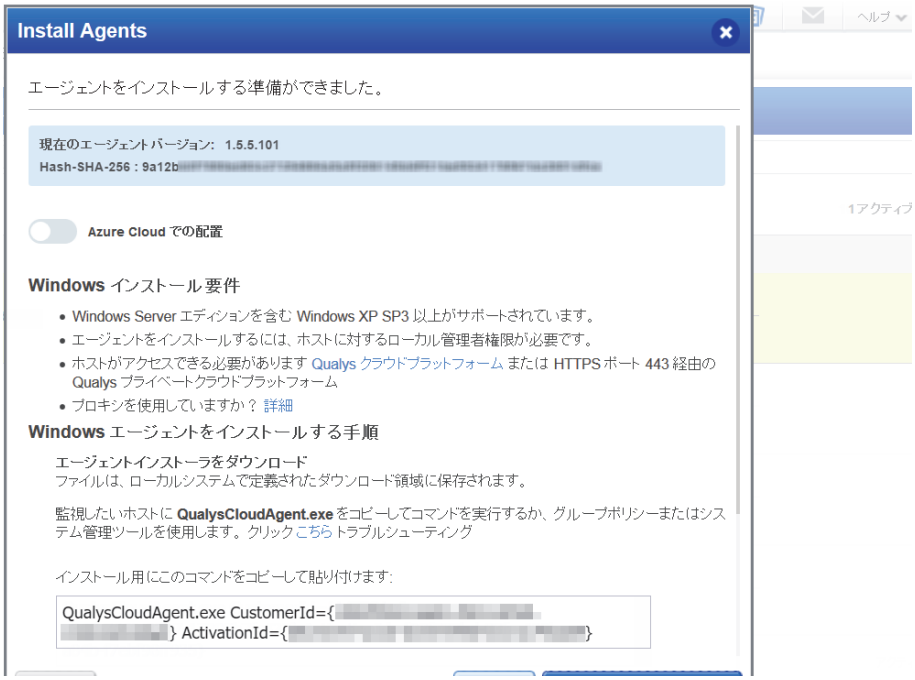
一定のエージェント数または特定の日付、あるいはその両方が経過した後はキーの期限が切れるようするには、制限を設定します。

アカウントのアプリのエージェントを自動でアクティブ化します。後でエージェントをアクティブ化するにはこの手順をスキップします。

要件を確認 要件を確認してから、対象のエージェントホストの「インストール手順」をクリックします。

表示されないオプションがある場合は、「ヘルプ」→「サポートへのお問い合わせ」までご連絡ください。

エージェントをインストール エージェントインストーラをダウンロードしてホストで実行します。インストーラを実行するには、表示されているコマンドをコピーして貼り付けるだけです。



各ホストでコマンドプロンプトから昇格した権限でインストーラを実行するか、またはグループポリシー あるいはシステム管理ツールを使用します 。

プロキシ対応の設定 これらのオプションやほかのオプションについては、インストールガイドが役に立ちます。

インストールガイド : Windows エージェント | Linux エージェント | Unix エージェント | Mac エージェント

AWS でのエージェントのインストール

下記のリンクに示されているインストール手順に従ってください。

詳細

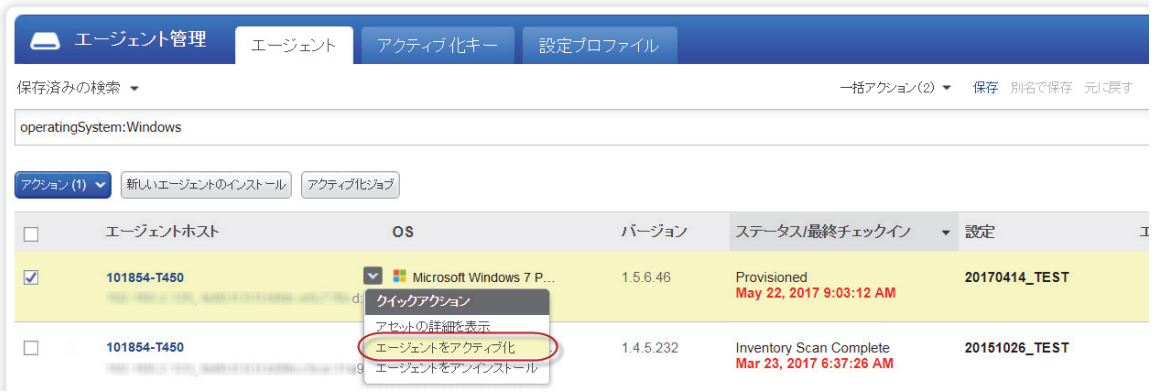
AWS での Cloud Agent のインストール

アセットデータをクラウドに同期！

エージェントはクラウドエージェントプラットフォームに即時接続して登録します。最初のアセット検出結果は数分で表示されるはずです。これはライトスキャンで、IP アドレス、OS、DNS/NetBIOS 名、MAC アドレスなどのアセットインベントリデータを収集します。

ステータスメッセージは継続的に更新されます。詳細

エージェントのアクティブ化（必須）モジュール（VM/PC）のエージェントをアクティブ化します。「クイックアクション」メニューから「エージェントをアクティブ化」を選択します（または「アクション」メニューを使って複数のエージェントを一括でアクティブ化します）。この手順をスキップすると、エージェントはインベントリ情報（IP アドレス、OS、DNS、NetBIOS 名、MAC アドレス）のみを同期し、クラウドエージェントプラットフォームはホストの評価とセキュリティ脅威の報告を実行しません。



エージェントのステータスがありませんか？インストール後数分でエージェントのステータスが（「エージェント」タブ上に）表示されます。ステータスが表示されない場合、エージェントがインストールされておらず、クラウドプラットフォームに正常に接続されず登録されていないことを意味します。

この理由としてよくあるものは次の 2 つです。

1) エージェントホストが Qualys クラウドプラットフォーム（または該当する場合は Qualys プライベートクラウドプラットフォーム）に HTTPS ポート 443 経由で接続できない。ネットワークアクセスを確認し、アカウントに表示されるプラットフォーム URL をホワイトリストに登録してください。詳細については、「ヘルプ」→「一般情報」を参照してください。

2) カスタムプロキシがある。「クイックスタートガイド」→「Cloud Agent の概要」を参照してください。

ヘルプが必要ですか？アセットデータとクラウドとの同期を開始するには、エージェントをクラウドプラットフォームに接続する必要があることに注意してください。ここをクリックしてトラブルシューティングを行います。

クラウドの継続スキャン

クラウドの最初の評価スキャンには少し時間がかかります。スキャン後、新規ホストメタデータがプラットフォームにアップロードされ、スキャンが完了します。

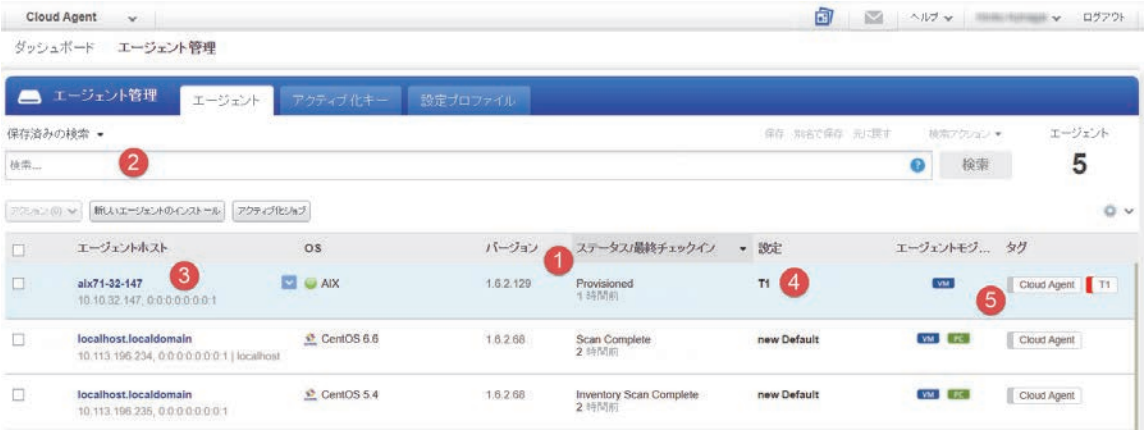
動作方法 エージェントはベースラインスナップショットのアップロードを評価のためクラウドエージェントプラットフォームに送信します。初回アップロードではエージェントがターゲットホストに関する総合メタデータ（数メガバイト）を収集し、ベースラインスナップショットを評価のためクラウドに送信します。正常に終了するとステータス「スキャン完了」が報告されます。この最初のスキャンは、デフォルト設定を使用して通常 30 分から 2 時間かかります。その後、デルタアップロード（それぞれ数キロバイト）に対してスキャンが即時実行されます。

エージェントが収集するアセットデータには、ベースラインスナップショットに対して、ネットワーク状態、OS、オープンポート、インストール済みソフトウェア、レジストリ情報、インストールされたパッチの種類、環境変数、ファイルに関連付けられたメタデータなどの多くの情報が含まれます。エージェントはスナップショットをエージェントホストに保存し、収集したホストメタデータに対するデルタを即時判定します。

テストされるシグニチャは？エージェントベースのスキャンは、従来の Qualys スキャナによるスキャンと同じシグニチャ（脆弱性、コンプライアンス、データポイント数）を使用します。VM に対してエージェントをアクティブ化している場合、脆弱性シグニチャをテストします。PC に対してエージェントをアクティブ化している場合は、コンプライアンスデータポイント数をチェックします。

エージェントの管理

エージェントの概要



1. インストールから数分以内にステータスメッセージが表示されます。詳細
2. エージェントの検索 - エージェントリストには、Qualys クラウドプラットフォームに接続されているインストール済みエージェントがすべて表示されます。
3. エージェントのホスト名 - Windows ホストの場合は NetBIOS 名、Linux ホストの場合は DNS 名。表示する名前を設定できます。「クイックアクション」メニューから「アセットの詳細を表示」を選択するだけです。
4. 設定プロファイルには、エージェントの動作に影響を与える設定があります。すぐに使用できるように、「Initial Profile」というプロファイルが用意されています。カスタマイズした設定のプロファイルを作成するには、「設定プロファイル」に移動し、「新規プロファイル」を選択します。
5. エージェントホストには、「Cloud Agent」タグが自動で割り当てられます。タグは、エージェントアセットの管理とレポート作成に役立ちます。

「クイックアクション」メニューでは次の操作が可能です。

- アセット詳細の表示
- さまざまな評価（VM、PC など）を行うためのエージェントのアクティブ化
- エージェントをアンインストール

「アクション」メニューは一度に複数のエージェントを更新できます。

エージェントのステータスについて

エージェントのステータスは継続的に更新され、エージェントに関する最新情報が常に提供されます。ステータスが表示されませんか？トラブルシューティングのヒントを参照してください（「ヘルプ」→「オンラインヘルプ」）。

セットアップ済み

エージェントはクラウドプラットフォームに正常に接続して登録されました。

マニフェストのダウンロード完了

クラウドプラットフォームはこのエージェントに割り当てられたマニフェストを更新しました。これでエージェントにどのメタデータをホストから収集するかを伝えます。更新されたマニフェストは正常にダウンロードされ、このエージェントに対して有効です。Windows　以外のエージェントの場合、「状態」カラムには、「インベントリ用にダウンロードされたインベントリマニフェスト」などの特定のマニフェストダウンロードステータスと、スキャンの次のステータスが表示されます。

「ダウンロードされた VM マニフェスト」、「ダウンロードされた PC マニフェスト」、「ダウンロードされた FIM マニフェスト」、「ダウンロードされた IOC マニフェスト」

設定のダウンロード完了

ユーザがこのエージェントに割り当てられた設定プロファイルを更新しました。これは、エージェントがホストからデータを収集する方法などエージェントの動作を定義します。更新されたプロファイルは正常にダウンロードされ、このエージェントに対して有効です。

エージェントのダウンロード完了

エージェントの新規バージョンがダウンロードされ、エージェントが自動更新プロセスの一環としてアップグレードされました。エージェントのアップグレードに再起動は不要です。

インベントリスキャン完了

エージェントがホストの検出を完了し、ホスト情報を収集してクラウドプラットフォームに送信しました。ホスト検出中にエージェントは IP アドレス、OS、NetBIOS 名、DNS 名、MAC アドレスなどの情報の収集を試行します。

スキャン完了

エージェントは新規ホストのメタデータをアップロードし、クラウドプラットフォームで評価が実行されました。新規評価データ（例えば新規 VM 脆弱性、PC データポイント）がある場合、クラウドプラットフォームはこのデータを処理して、アカウントで表示やレポートに使用できるようにします。

アクティブ化ジョブの進行状況の表示

エージェントのアクティブ化を開始すると、アクティブ化されるまでしばらく時間がかかる場合があります。アクティブ化ジョブの進行状況は簡単にチェックできます。

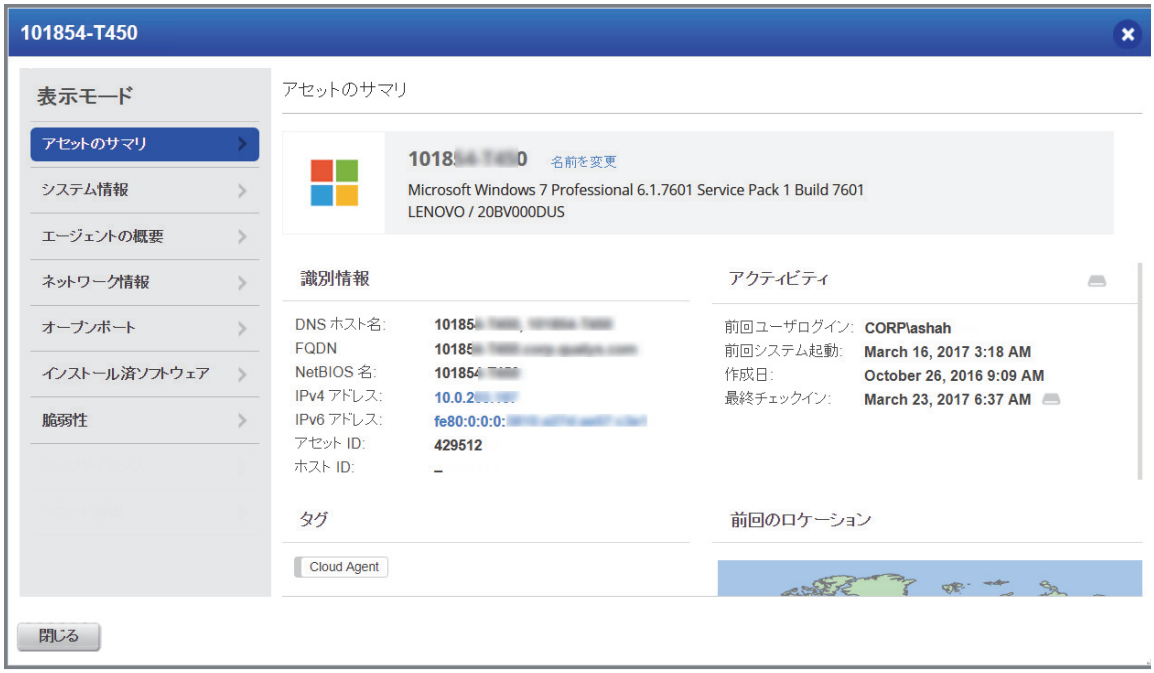
エージェントリストに移動し、「アクティブ化ジョブ」をクリックします。

開始されているアクティブ化ジョブのリストが表示されます。ジョブの進行中に、アクティブ化を停止 / キャンセルすることができます（必要に応じて、後でアクティブ化することもできます）。

現在のアセットの詳細を簡単に表示

「**アセットの詳細を表示**」をメニューから選択します。

「アセットのサマリ」とこれに続く項には、最新のインベントリスキャンおよび最新の完全スキャン（評価）から返された現在のアセットデータが表示されます。

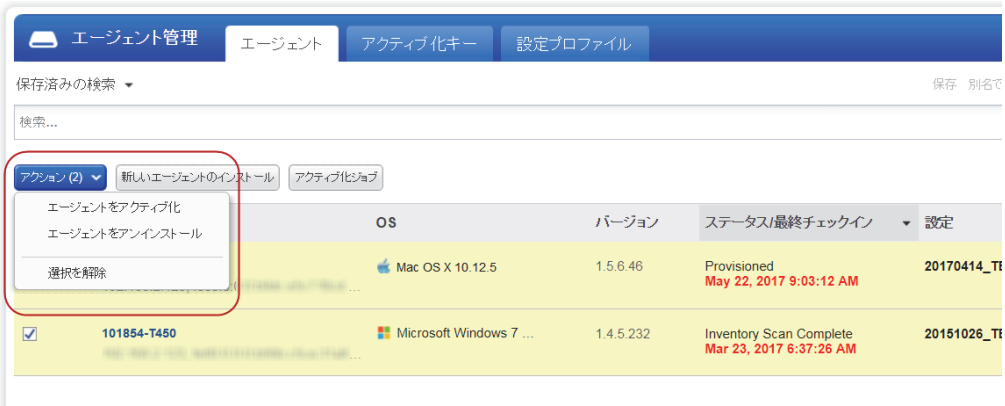


脆弱性評価から返された包括的な詳細を表示するには、各種の項をドリルダウンします。アカウントで Policy Compliance（PC）が有効な場合はコントロールデータポイントが表示され、Continuous Monitoring（CM）が有効な場合はアラート通知が表示されます。

エージェントへの一括アクション

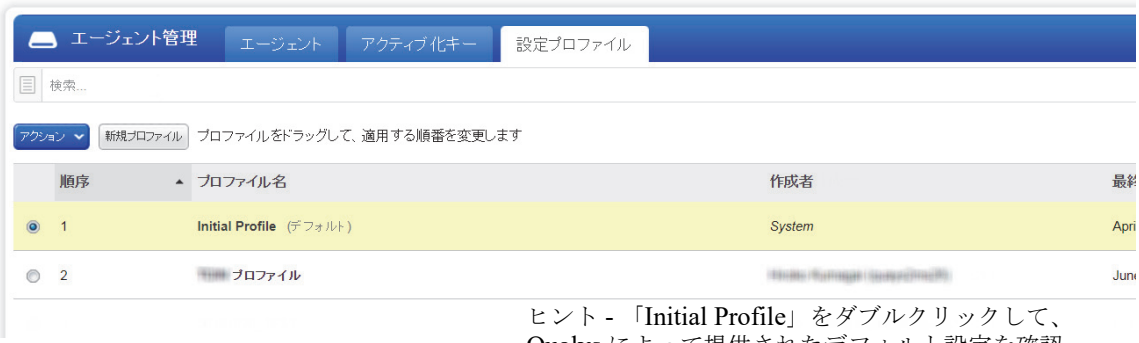
一度に複数のエージェントをアクティブ化、非アクティブ化、アンインストールします。

エージェントリストからエージェントを選択し、「アクション」メニューを開き、適用する一括アクションを選択します。



設定の変更

エージェントにはデフォルト設定があり、これがエージェントの動作をコントロールします。設定プロファイルを作成してエージェント設定を変更したり、適用順を変更したりできます。



ヒント - 「Initial Profile」をダブルクリックして、Qualys によって提供されたデフォルト設定を確認

「**Initial Profile**」は Qualys によって提供された設定のデフォルトプロファイルです。これはインストール時にデフォルトでエージェントに割り当てられています。プロファイル設定は簡単に表示できます。

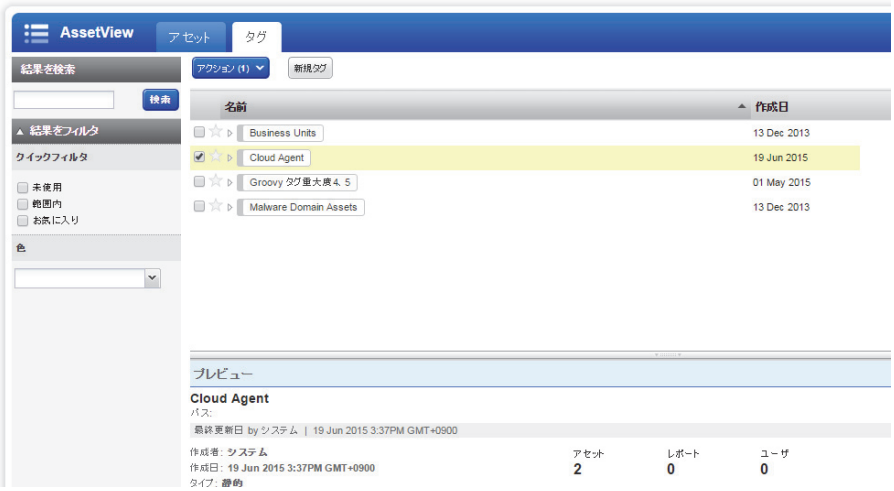
「**プロファイル設定**」は多くのエージェントの動作に影響します。エージェントがメタデータを収集する方法とタイミング、クラウドプラットフォームと同期するタイミング、自動更新のタイミング、パフォーマンスのチューニング、帯域の使用などです。カスタムプロファイルを作成し、ホストに割り当てることができます。

ベストプラクティス ノートパソコン、サーバ、デスクトップ、データセンタなどネットワークインフラの異なるパーツに異なるエージェント設定を割り当てることがあります。そのためには、グループ化に従ってホストにタグ付けし、そのタグを異なる設定プロファイルに割り当てます。

エージェントホストのタグ付け

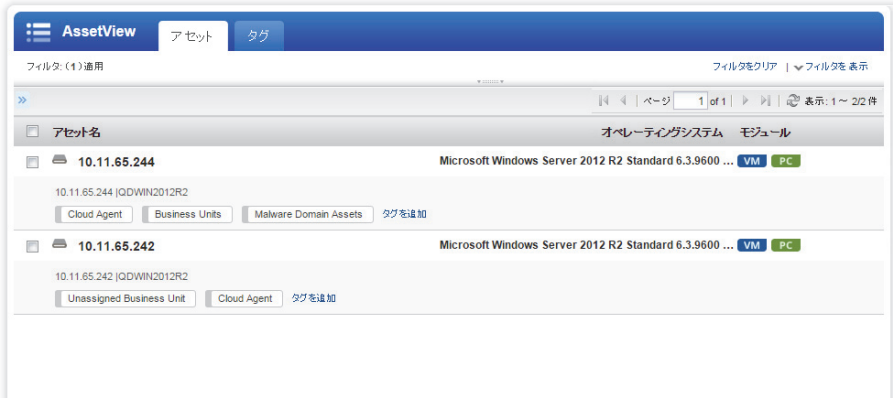
動的アセットタグ付け機能は、エージェントホストのアセットをサブスクリプション内のその他のアセットと同じように管理できるようにします。

「Cloud Agent」タグはすべてのエージェントホストに割り当てられます。このタグを選択すると、エージェントホスト（アセット）の数が表示されます。



「アセットを検索」オプションではエージェントアセットを検索できます。

エージェントホストにタグ付けして整理し、レポートすることもできます。



エージェントファイルを検索していますか？

エージェントはクラウドプラットフォームによって一元管理されます。このため、ホストにインストールしたエージェントファイルは編集または実行しないでください。参考のため、該当するエージェントファイルをここに示します。トラブルシューティングに役立てるには、ログファイルを確認します。

その内容は？プログラムファイル、マニフェスト（エージェントが収集するデータに関する手順）、設定（エージェントの動作方法）、スナップショットデータベース、ログファイルです。

Windows エージェント

C:\Program Files (x86)\QualysAgent\Qualys\QualysCloudAgent.exe
C:\Program Files (x86)\QualysAgent\Qualys\Uninstall.exe
C:\ProgramData\Qualys\QualysAgent*

ログファイル（Log.txt、Archive.txt）は次の場所にあります。
C:\ProgramData\Qualys\QualysAgent

XP および Server 2003 では、ログファイルは次の場所にあります。
C:\Documents and Settings\All Users\Application Data\Qualys\QualysAgent

カスタム変数がありますか？ご心配は要りません。ホストに定義された環境設定に従ってエージェントをインストールします。

Linux エージェント、Unix エージェント、Mac エージェント

/etc/init.d/qualys-cloud-agent
/etc/qualys/cloud-agent/qagent-log.conf
/var/log/qualys/qualys-cloud-agent.log
/usr/local/qualys/cloud-agent/* //Linux, Unix
/Applications/QualysCloudAgent.app/* //MacOS

ヘルプが必要ですか？ここをクリックしてトラブルシューティングを行います。

Qualys プラットフォームアプリケーションの使用

エージェントがホストの問題を検出するとすぐに通知されます！

Qualys クラウドプラットフォームアプリケーション（VM、PC、AV、CM など）は、エージェントが収集した脆弱性管理データとポリシーコンプライアンスデータを自動的に統合します。エージェントからクラウドプラットフォームへ報告された変更は即時評価され、更新されたアセットデータはすぐにアカウントで使用可能になります。

Qualys アプリケーションは以下の情報を提供します。

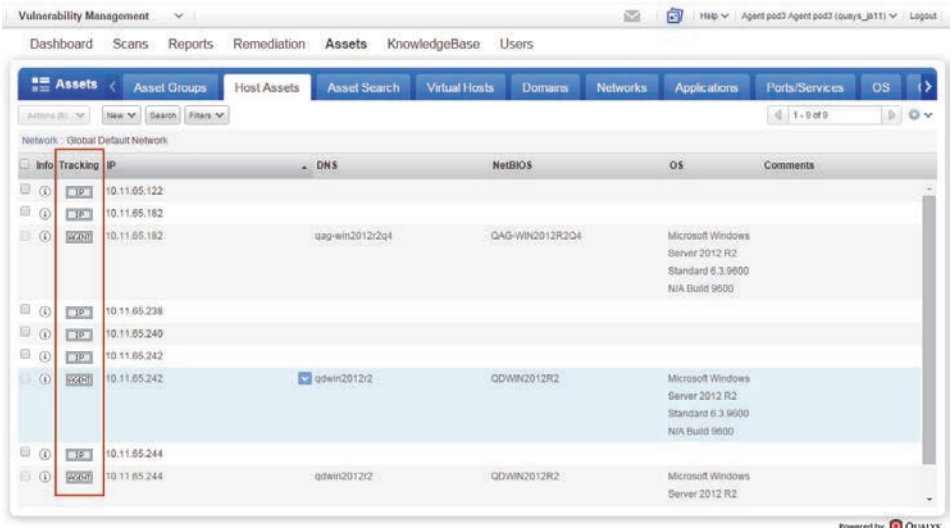
- ホストに対する最新のセキュリティ状態
- 分単位の評価およびセキュリティ上の脅威の詳細
- 最新アセットデータのレポートおよびアセットデータのスケジュール機能
- 特定のホスト変更の発生と同時にアラート（Continuous Monitoring を使用）

最新のセキュリティ更新を取得するために、いつでもアカウントに移動できます。

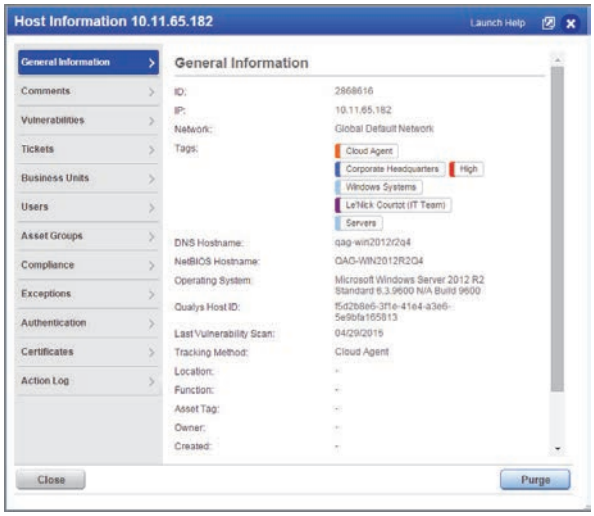
Vulnerability Management

最新の Vulnerability Management 評価データは、クラウドエージェントプラットフォームが実行するスキャンから常時提供され、Qualys アカウントで使用可能です。

「Host Assets」タブには、追跡方法が「Agent」のエージェントホストが表示されます。



ⓘ をクリックすると包括的なホスト情報が表示されます。



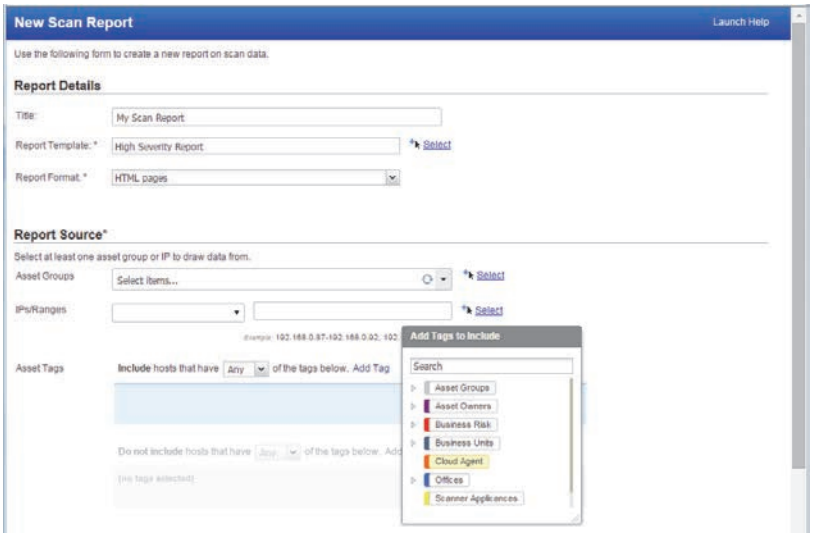
ライトスキャンが完了すると、エージェントホストに関する基本情報が表示されます。

このホストについては、すでに Asset Management アプリケーションを使ってタグを追加しています。

VM 評価データはエージェントホストの「Vulnerabilities」項に表示されます。これは別の追跡方法で追跡された従来のホストと同様です。

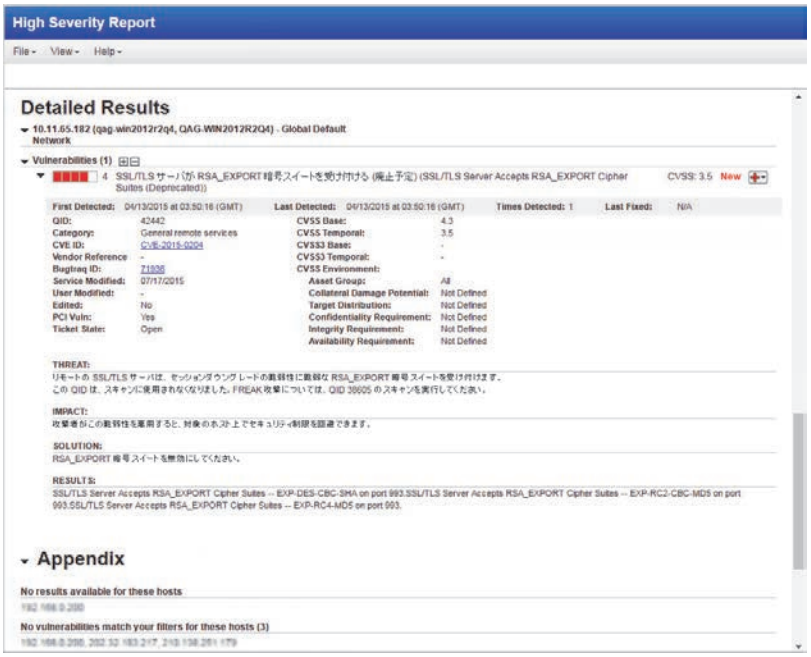
フルスキャンが完了すると、「Vulnerabilities」項に評価データが表示されます。

必要に応じて最大で分単位の評価データを含むエージェントホストに関する VM レポートを作成するか、都合のよい時間に実行するようスケジュールすることができます。



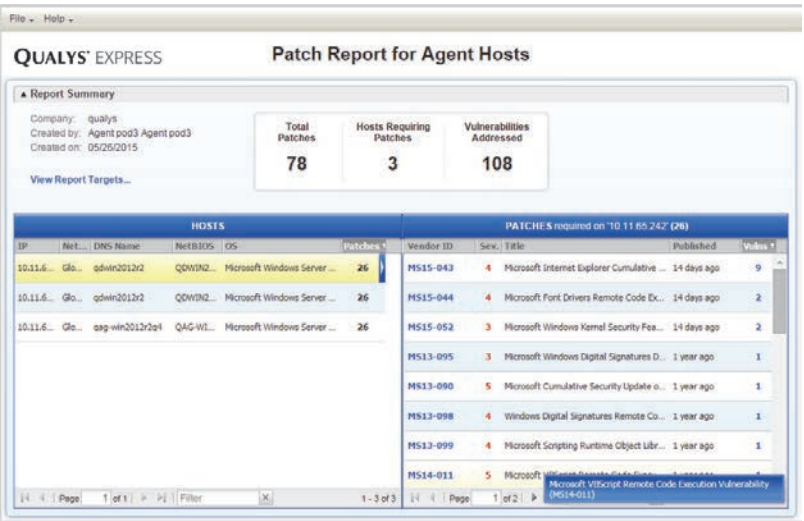
ヒント - 「Cloud Agent」タグを選択してすべてのエージェントホストについてレポートすることができます。

この例では、「High Severity Report」にエージェントホストの詳細結果が表示されています。詳細はサブスクリプション内の他のホストと同じように表示されます。



このレポートの実行方法「VM」→「Reports」→「Templates」に進んで「High Severity Report」を選択し、「Quick Actions」メニューから「Run」を選択します。

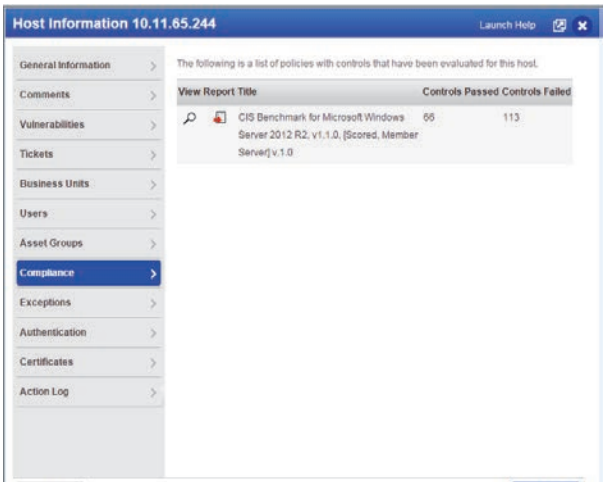
これは「Patch Reports」でも同じです。パッチレポートを実行してエージェントホストに必要なパッチを検出することができます。これは IP アドレス、NetBIOS、または DNS で追跡されるホストと同様です。レポート対象に「Cloud Agent」タグを選択すると、レポートにはアカウント内のすべてのホストエージェントが含まれます。



このレポートの実行方法「Reports」→「Report Templates」に進んで「Qualys Patch Report」を選択し、「Quick Actions」メニューから「Run」を選択します。

Policy Compliance

最新のポリシーコンプライアンス評価データは、クラウドエージェントプラットフォームが実行するスキャンから常時提供され、Qualys アカウントで使用可能です。「Host Assets」タブには、追跡方法が「Agent」のエージェントホストが表示されます。



フルスキャンが完了すると、「Compliance」項では、ポリシーの一覧とともに、ホストに対して評価されたコントロールが表示されます。

- 必要に応じて最新のアセットデータを含むエージェントホストに関する PC レポートを作成するか、都合のよい時間に実行するようスケジュールする
- 最新の個別ホストコンプライアンスレポート（pdf）を「Host Information」からダウンロード
- アカウント内のエージェントホストのレポート対象として「Cloud Agents」タグを選択

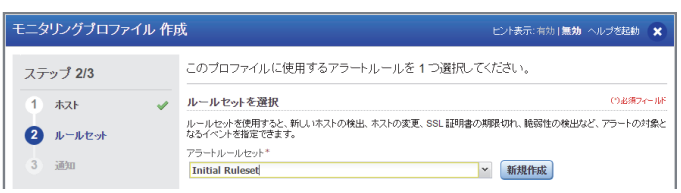
Continuous Monitoring

Continuous Monitoring を使用すると、サブスクリプション内の他のホストと同様に、エージェントホストで変更が発生してから数分以内にアラートを受信することができます。ここでは、簡単に開始する方法を説明します。

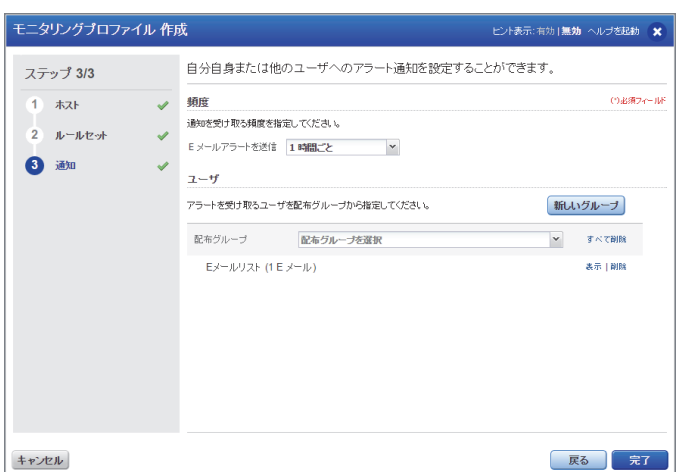
「設定」→「モニタリングプロファイル」に移動し、「新規プロファイル」を選択します。

タグまたは「IP/ 範囲」を選択してエージェントホストを選択します。

ヒント - アカウントの IP ネットワーク範囲のタグ (AssetView を使って定義されたカスタムアセットグループ、ビジネスユニット、またはカスタムタグなど) から選択します。



最初は「Initial Ruleset」を使用することをお勧めします。(これは今すぐカスタマイズすることも、後で行うこともできます)



通知オプションで頻度と配布グループを設定します (忘れずにご自分を通知先に含めてください)。

これで完了です！エージェントホストに関するアラートを受信できるようになりました。ルールセットやプロファイルはいつでも更新して、アラート対象やタイミングを変更することができます。