Qualys AssetView

ユーザガイド

2020 年 4 月 3 日

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

Qualys AssetView へようこそ。AssetView は、Qualys が無償で提供するアセット検出およびインベントリサービスです。これを使用すると、すべてのアセットを 1 か所ですぐに表示できます。

Qualys について

Qualys, Inc.（NASDAQ: QLYS）は、セキュリティとコンプライアンスを目的とするクラウド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、Deutsche Telekom、富士通、HCL、HP Enterprise、IBM、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。オンラインサポートの情報については、www.qualys.com/support/ をご覧ください。

はじめに

Qualys AssetView を使用すると、常時更新されるネットワークをまとめて表示することができます。

対象となるアセット

Qualys 外部スキャナ、Scanner Appliance、Cloud Agent を使用してスキャンされたすべてのアセット（IP アドレス、Web サイト）が表示されます。アセットが表示されない場合は、スキャンを開始するか、エージェントをインストールしてください。

スキャンの開始

アプリケーションの VM/VMDR、PC、WAS を使用してスキャンを設定します。スキャン結果が処理されると、アセットインベントリが更新されます。WAF を使用している場合は、WAF を使用して Web サイトにファイアウォールを設定します。

ヒント - アカウントに新しいデータセキュリティモデルを設定する必要があります。設定が完了していることを確認します。これは、マネージャが「VM/VMDR」→「Users」→「Set Up」→「Security」を選択して設定します。

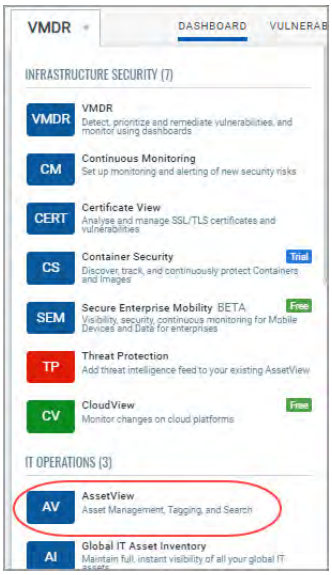
エージェントのインストール

アプリケーションピッカーから Cloud Agent（CA）を選択すると、手順が表示されます。所要時間は数分ほどです。エージェントは、自社運用のシステムにも、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、自動管理および自動更新されます。

アセットの検索

アセット項の検索フィールドを使用すると、スキャンおよび Cloud Agent から返されるすべてのアセットデータを瞬時に、適切かつ柔軟に検索できます。

まず、アプリケーションピッカーから AssetView を選択します。



(「アセット」タブの)「アセット」ダッシュボードの上に検索フィールドが表示されます。ここに検索クエリを入力します。

入力を開始すると、ユーザ名、ホスト名などの検索可能なアセットプロパティが表示されます。目的のアセットプロパティを選択します。

Threat Protection ユーザへのヒント：

脅威を入力すると、Real-time Threat Indicator (RTI) が表示されます。

一致させたい値を入力し、「検索」をクリックします。アセットリストに、一致した内容が表示されます。

ヒント：

「ダッシュボード」タブで、クエリを使用してダッシュボードウィジェットを作成できます。

グループ化オプション

アセットの検索結果を取得したら、その結果を論理グループに分類することができます。オペレーティングシステム、オープンポート、DNS アドレス、タグ、脆弱性などのグループ化オプションがあります。

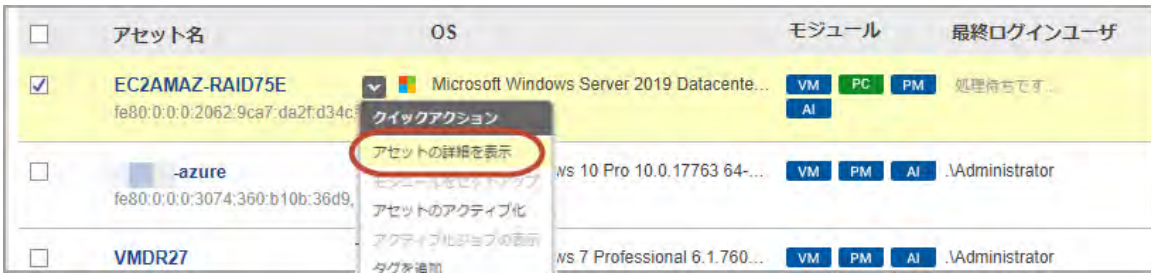
アセット検索クエリを入力し、アセット検索結果を取得します。次に、「項目別にアセットをグループ分け...」ドロップダウンからグループ化オプションを選択します。

選択した内容に基づいて固有グループの数（28 の固有オペレーティングシステムなど）とグループごとのアセット数が表示されます。任意のグループをクリックすると、検索クエリが更新され、一致するアセットが表示されます。

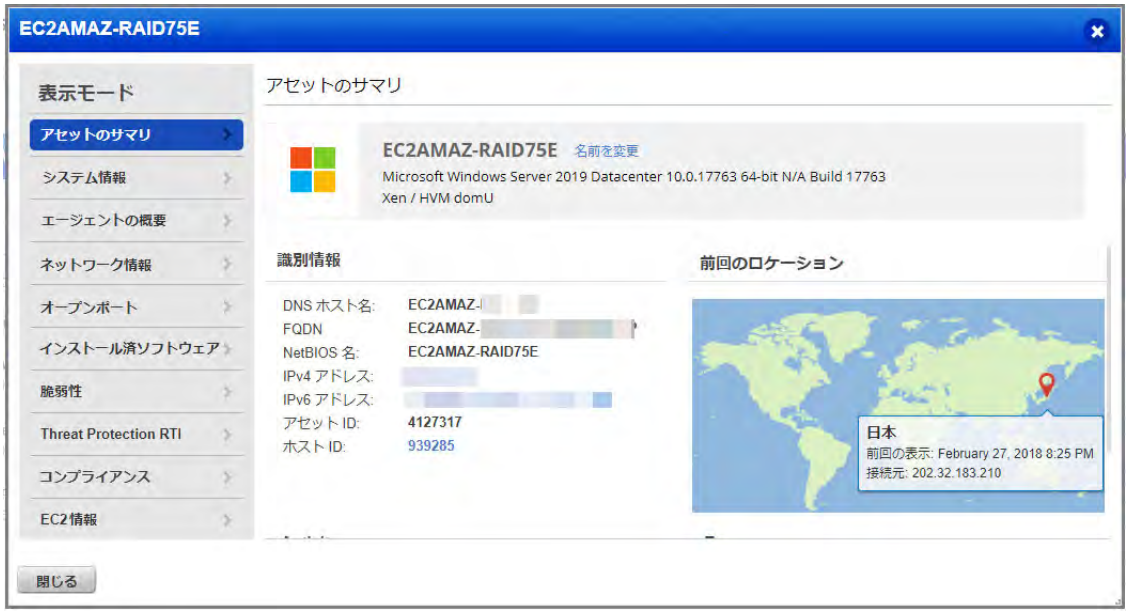
ダッシュボードウィジェットのグループ化オプションを使用することもできます。例えば、このウィジェットは、DNS アドレスでグループ化されています。

アセットの詳細をいつでも表示

特定のホストアセットのセキュリティおよびコンプライアンス状態を把握できるよう詳細を表示します。対象のアセットを選択し、メニューから「アセットの詳細を表示」を選択します。



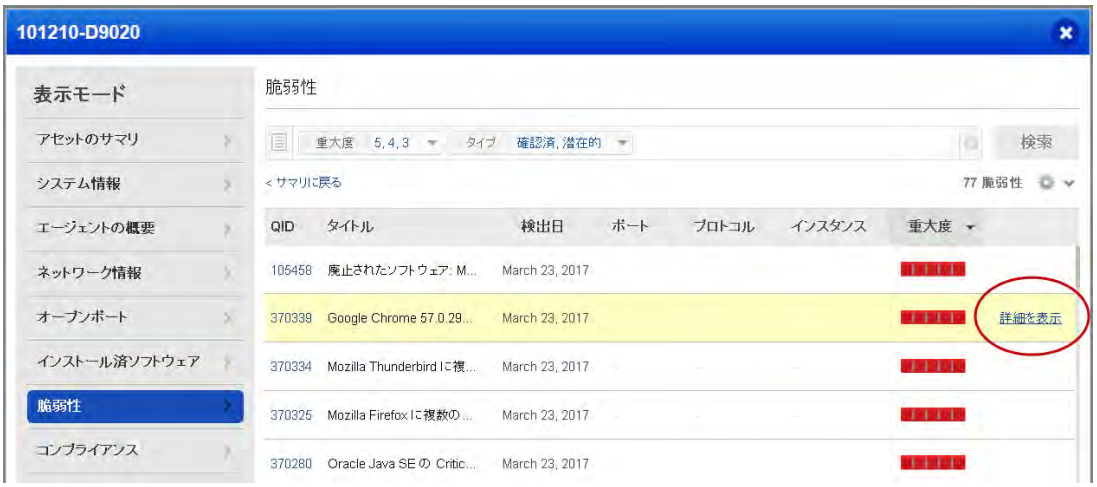
左側の項を選択すると、アセットの詳細が表示されます。



「脆弱性」で「脆弱性を表示」をクリックすると、アセットの脆弱性が表示されます。

ここから、脆弱性を検索できます。オプションをクリックすると、カスタムフィルタ（QID、タイトル、検出日など）を適用できます。デフォルトでは、無視されたすべての脆弱性はここに一覧表示されます。「無視」オプションを使用して、無視された脆弱性の表示と非表示を切り替えます。

「詳細を表示」をクリックすると、リスト内の任意の QID の最新検出結果が表示されます。



新しい「コンプライアンス」タブで、アセットのすべてのポリシーコンプライアンスサマリを表示します。ここには、このアセットが関連付けられているコンプライアンスポリシーと、そのポリシーがこのアセットに対する安全な設定コントロールに関連してどのように動作するかが表示されます。（このタブは、アセットで PC アプリケーションが有効化されている場合にのみ表示されます）。

さらに、サブスクリプションの設定に応じて、その他のタブが表示される場合があります。

例：

Threat Protection RTI - アセットの Real-time Threat indicator（RTI）と関連する脆弱性を表示します（このタブは、アセットで TP アプリケーションが有効化されている場合にのみ表示されます）。

「アラート通知」- Continuous Monitoring を使用して設定したアラートルールセットに基づいて、アセットの対象の脆弱性に対するアラート通知を表示します。（このタブは、アセットで CM アプリケーションが有効化されている場合にのみ表示されます）。

アセットの位置の特定

パブリック IP を使用して、アセットの位置情報を追跡します。米国のユーザにはデフォルトでアセットの位置情報サービスが有効になっています。パブリック IP が関連付けられているアセットでは、「アセットの詳細」→「アセットのサマリ」の世界地図に最新の位置が表示されます。

アセットの位置情報を有効化（または無効化）するには、Qualys サポートまたは Qualys アカウントマネージャにお問い合わせください。

動作方法

- アセットのネットワークインタフェースのパブリック IP がチェックされます。

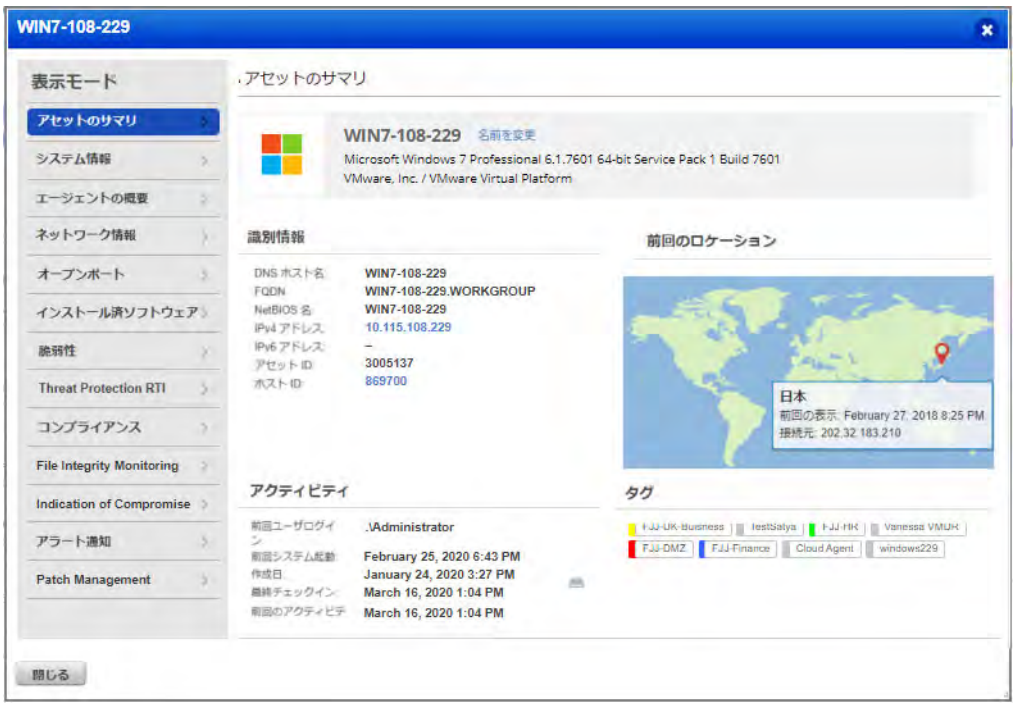
- エージェントがインストールされているアセット - エージェントがレポートした IP がチェックされます。

- AWS/EC2 アセット - EC2 インスタンスのパブリック IP が使用されます。

- ネットワークに関連付けられているアセット - 使用されているスキャナに関連付けられているパブリック IP が検索されます 。

- パブリック IP が見つからない場合、位置情報は不明と表示されます。

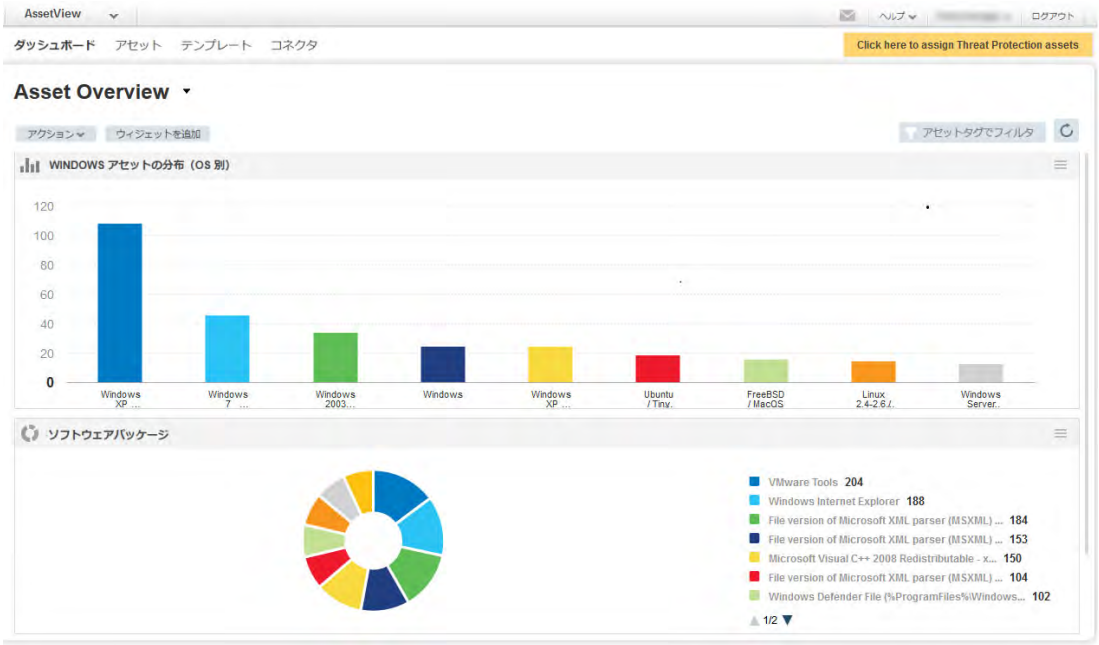
以下の例では、アセットの最新位置は、1 分前のカリフォルニア州レッドウッドシティです。



動的ダッシュボード

ダッシュボードを使用すると、アセットを視覚化し、改善が必要な脆弱性に対し優先順位付けができます。検索クエリを持つウィジェットを追加して、対象を明確に表示します。「アクション」メニューから、ダッシュボードおよびウィジェットの設定を JSON 形式でファイルにエクスポートおよびインポートすることもできます。これにより、アカウント間または Qualys コミュニティ内でウィジェットを共有できます。

複数のダッシュボードを作成して、データ表示に応じて切り替えます。



ダッシュボードの管理には、「アクション」メニューを使用します。

ウィジェットの追加

1）ダッシュボードの「ウィジェットを追加」ボタンをクリックします。

2）ウィジェットテンプレートの 1 つを選択します。選択できるウィジェットテンプレートは数多くあります。また、独自のウィジェットを作成することもできます。

3）それぞれのウィジェットは異なっています。アセットデータ、クエリ、レイアウト（カウント数や表、棒グラフ、円グラフなど）を選択するものもあります。

4）「アクション」メニューから、ウィジェットの設定を JSON 形式でファイルにインポートおよびエクスポートすることもできます。これにより、アカウント間または Qualys コミュニティ内でウィジェットを共有できます。

ヒント：

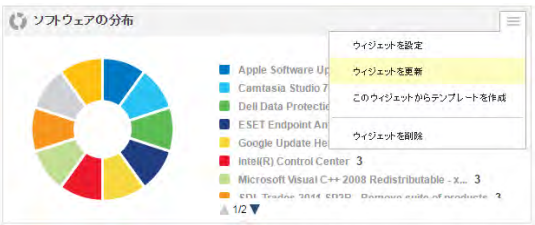
- デフォルトのダッシュボードに作成されたウィジェットでは、「アクション」→「ウィジェットを設定」を選択して設定を表示します。

- ウィジェットの縦横のサイズを変更したり、ページ上でウィジェットをドラッグアンドドロップして、レイアウトを変更したりできます。

- チャートの項をクリックすると、アセットインベントリに一致するアセットが表示されます。

表示の更新

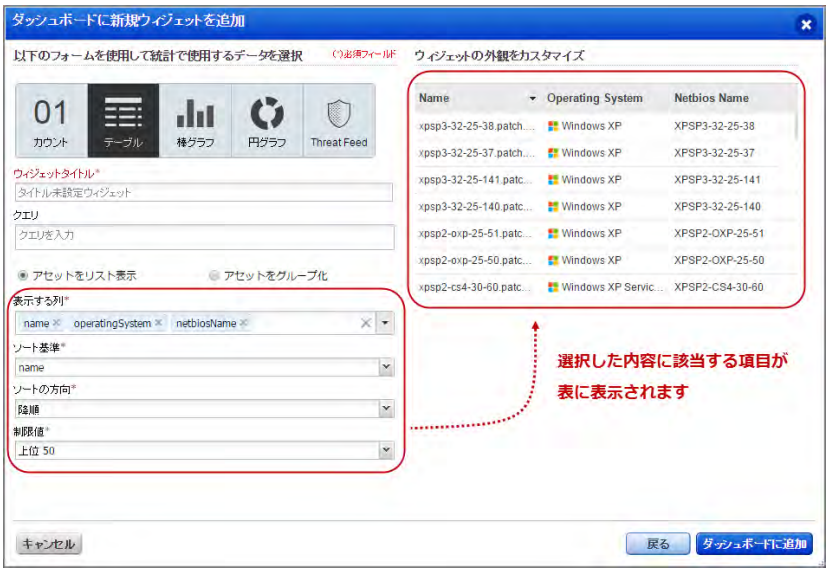
ウィジェットの最新アセットデータを表示できます。ウィジェットタイトルの右側のラベルを選択し、ウィジェットメニューから「ウィジェットを更新」を選択します。



すべてのウィジェットを一度に更新するには、「すべて更新」をクリックします。すべてのウィジェットが更新されます。

ウィジェットへのテーブルの追加

アセットとそのセキュリティの視覚化に役立つテーブルをウィジェットに設定する方法がいくつかあります。複数の列を設定したテーブルを作成したり、列ごとにソートしたり、ソート順（昇順または降順）を設定したりします。



トレンドデータの表示

ダッシュボードのカウントウィジェットを設定して、トレンドデータを表示します。動的ウィジェットウィザードで「トレンドデータを収集」を有効化します。有効にすると、ウィジェットのトレンドデータが毎日収集され、最大 90 日間保存されます。これは、カウントウィジェットの折れ線グラフを作成するときに使用されます。

テンプレートについて

ダッシュボードまたはウィジェットを新規作成するときの最初の手順として、ライブラリからテンプレートを選択します。ライブラリには、システムが提供するテンプレートとユーザが作成したテンプレートが表示されます。

「テンプレート」項では、ライブラリでのテンプレートの表示方法を変更できます。次の操作が可能です。

- テンプレートの名前変更

- テンプレートの説明の更新

- テンプレートをリストから削除

変更または削除できるテンプレート

自分が作成したテンプレートは操作できます。システムテンプレートは編集も削除もできません。

アセットへのタグの適用

タグを設定して、サブスクリプションのアセットにタグを適用できるようにします。これにより、アセットを整理し、アセットへのユーザのアクセスを管理できます。IP アドレスおよび Web アプリケーションにタグを適用できます。

タグの設定

1)「タグ」を選択し、「新規タグ」を選択します。

2) タグの設定を入力します。ヒント - ウィザードのタイトルバーでヒント表示をオンにすると、設定にマウスポインタを置いたときにヘルプが表示されます。

3) 動的タグルールを設定します(オプション)。動的ルールがない場合、タグは静的タグとして保存されます。

タグを動的タグルールで保存すると、定義したルールに一致するすべてのスキャン済みホストにそのタグが割り当てられます。ルールに一致するアセットのみを表示するように、アセットリストをフィルタリングができます。

自動定義のタグ

特定のタグは自動的に作成されます。

Business Units

アカウント内のビジネスユニットに対して、サブタグを持つ「Business Units」タグが作成されます。ビジネスユニット内のアセットは、自動的にそのビジネスユニットのタグに割り当てられます。

サブタグは以下のとおりです。

- Unassigned Business Unit

- アカウントでカスタムビジネスユニットが定義されている場合、カスタムビジネスユニット名

Asset Groups

アカウント内のアセットグループに対して、サブタグを持つ「Asset Groups」タグが作成されます。アセットグループ内のアセットは、自動的にそのアセットグループのタグに割り当てられます。例えば、アカウントに West Coast という名前のアセットグループがある場合、「West Coast」という名前のタグが付与されます。

Cloud Agent

アカウント内の Cloud Agent に対して、サブタグを持つ「Cloud Agent」タグが作成されます。すべての Cloud Agent には、デフォルトで自動的に「Cloud Agent」タグが割り当てられます。

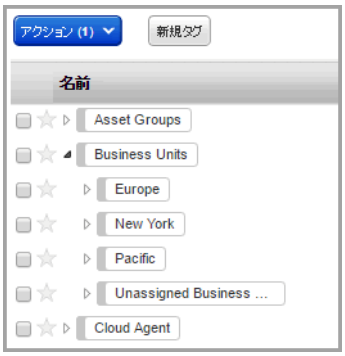
サブタグは以下のとおりです。

- 位置固有のエージェント

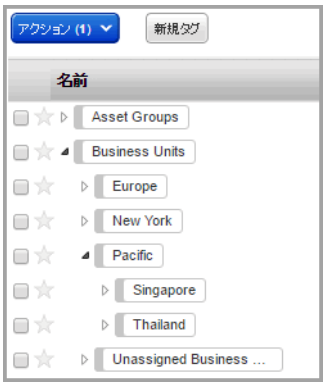
- マシン固有のエージェント

タグツリーについて

AssetView（AV）およびサブスクリプション内のアプリケーションにタグツリーが表示されます。ツリー内の上位レベルのアセットタグは、ツリーの最上位レベルに「Business Units」タグ、「Cloud Agent」タグ、「Asset Groups」タグのように表され、これらのビジネスユニット、Cloud Agent、アセットグループ内の個別のサブタグはタグツリーの枝として表されます。



タグを追加して割り当てながら、企業内の組織の関係をこのツリー構造で模倣していくことで、アセットの管理が容易になります。



タグツリーの利点は、ツリーにある任意のタグをスキャンまたはレポートに割り当てられることにあります。例えば、スキャン対象として「Pacific」を選択した場合、ユーザのスコープ内で「Pacific」がタグ付けされているアセットと、ユーザのスコープ内で「Thailand」および「Singapore」という「Pacific」のサブタグがタグ付けされているすべてのアセットが自動的にスキャンされます。

タグを持つアセットの検索方法

高度なアセット検索を使用します。例えば、「Windows All」というタグを持つアセットを見つけるには、「アセット」タブを選択し、検索クエリの tags.name に「Windows All」と入力します。次に「検索」をクリックして結果を表示します。

クラウドインスタンスのタグ

所属するクラウドプロバイダに従って、クラウドアセットを簡単にグループ化できます。Cloud Agent（AWS、AZURE、GCP）およびコネクタが検出したアセットにタグが適用されます。

クラウドコネクタが収集したメタデータに基づいて、タグクラウドインスタンスに適用する動的タグルールを作成します。タグルールごとに、インスタンス情報を指定した検索クエリを指定します。

手順：

1)「アセット」→「タグ」を選択し、「新規タグ」を選択します。

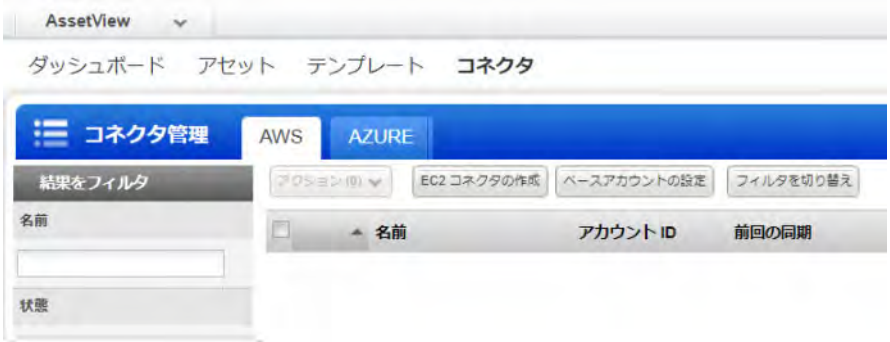
2)「クラウドアセット検索」タグルールを選択します。

3)「クラウドプロバイダ」AWS（EC2）、GCP、または AZURE を選択します。

4)「クエリ」フィールドに検索クエリを入力します（以下の例では、AWS/EC2）。使用できる一般的な検索クエリについては、オンラインヘルプを参照してください。

コネクタの設定

コネクタを設定すると、クラウドアカウントに存在するリソースの検出が開始されます。



AWS

Qualys クラウドプラットフォームを使用して、EC2 インスタンスのセキュリティ問題をスキャンするよう EC2 コネクタを設定します。「コネクタ」タブを選択し、「EC2 コネクタの作成」を選択すると、ARN 認証の設定、EC2 リージョンの選択、EC2 アセットのスキャンのためのアクティブ化、の各手順が表示されます。

ヒント - 少なくとも 1 つの汎用アセットタグ（EC2 など）を作成し、コネクタがそのタグをすべてのインポート済みアセットに自動で適用するようにすることをお勧めします。検出された EC2 メタデータに基づいて、EC2 アセットにタグを追加できます。

ビデオシリーズを見る | ユーザガイドのダウンロード

Azure

Qualys クラウドプラットフォームを使用して、Microsoft Azure リソースのセキュリティ問題をスキャンするよう Azure コネクタを設定します。「コネクタ」→「Azure」タブを選択し、「Azure コネクタを作成」を選択すると、ウィザードに手順が表示されます。

ヒント - 少なくとも 1 つの汎用アセットタグ（Azure など）を作成し、コネクタがそのタグをすべてのインポート済みアセットに自動で適用するようにすることをお勧めします。検出された Azure メタデータに基づいて、Azure アセットにタグを追加できます。