Qualys による Amazon Web Services の保護

2023 年 10 月 27 日

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

このガイドについて

Qualys Cloud Platform とクラウドでのセキュリティスキャンへようこそ。Qualys Cloud Security Platform を使用してクラウド IT インフラストラクチャをスキャンするための Qualys ソリューションについて理解を深めるお手伝いをします。

Qualys について

Qualys, Inc.(NASDAQ:QLYS)は、クラウドベースのセキュリティおよびコンプライアンスソリューションのパイオニアであり、リーディングプロバイダーです。Qualys Cloud Platform とその統合アプリは、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、保護の全範囲を自動化することで、企業がセキュリティ運用を簡素化し、コンプライアンスのコストを削減するのに役立ちます。

1999 年に設立された Qualys は、アクセンチュア、BT、コグニザント・テクノロジー・ソリューションズ、ドイツテレコム、富士通、HCL、HP Enterprise、IBM、インフォシス、NTT、Optiv、SecureWorks、タタ・コミュニケーションズ、ベライゾン、ウィプロなどの大手マネージド・サービス・プロバイダーやコンサルティング組織と戦略的パートナーシップを結んでいます。また、Cloud Security Alliance(CSA)の創設メンバーでもあります。詳細については、www.qualys.com をご覧ください。

Qualys サポート

Qualys は、徹底したサポートを提供することをお約束します。Qualys は、オンラインドキュメント、電話によるヘルプ、および直接の電子メールサポートを通じて、お客様の質問に可能な限り迅速に回答できるようにします。週 7 日 24 時間体制のサポートを提供しており、https://www.qualys.com/support/でサポート情報にアクセスする事ができます。

ご紹介

Qualys Cloud Platform は、従来の IT インフラストラクチャだけでなく、クラウド IT インフラストラクチャを保護するためのソリューションを提供します。このガイドでは、Qualys を使用して Amazon AWS EC2 インフラストラクチャを保護する方法について説明します。

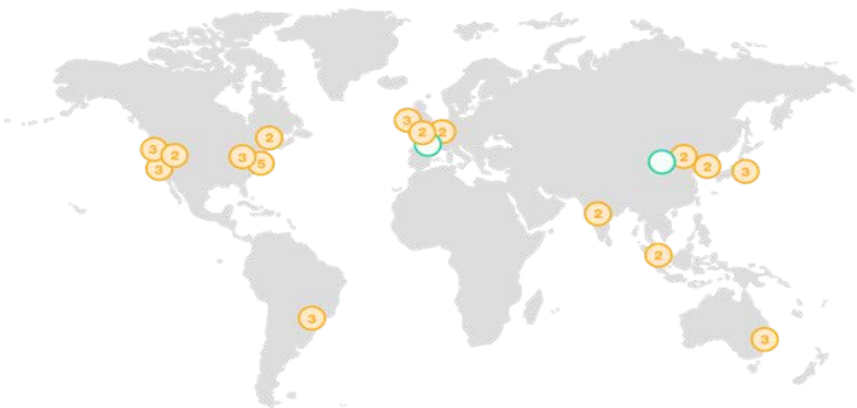
Qualys 統合セキュリティプラットフォーム

Qualys Cloud Platform を使用すると、セキュリティとコンプライアンスをリアルタイムで一元的に把握できます。Qualys を初めて使用する場合は、Qualys クラウドプラットフォームの Web ページにアクセスして、クラウドプラットフォームの詳細を確認することをお勧めします。

AWS の Qualys サポート

Qualys AWS クラウドサポートは、次の機能を提供します。

- EC2 インスタンス(IaaS)を脆弱性から保護し、OS の規制コンプライアンスを確認する
- アプリケーション(データベース、ミドルウェア)の継続的なセキュリティの確保
- Cloud Agents を AMI に埋め込んで、完全な可視性を得る
- 公開されている IP と URL の脆弱性を特定する
- アプリケーションスキャンおよびファイアウォールソリューションを使用したアプリケーションの保護
- 脆弱性スキャン
- GovCloud を含むすべての AWS グローバルリージョンをサポート
- Classic および VPC プラットフォームで EC2 インスタンスをサポート
- EC2 で動作することが認定された Qualys クラウドエージェント



Qualys センサー

Qualys Cloud Platform のコアサービスである Qualys センサーは、グローバル企業全体にセキュリティを簡単に拡張できるようにします。これらのセンサーは、リモートで展開でき、一元管理され、自己更新が可能です。データを収集し、Qualys Cloud Platform に自動的に送信し、Qualys Cloud Platform は、脅威の特定と脆弱性の排除を支援するために、情報を継続的に分析して関連付けるコンピューティング能力を備えています。

仮想 Scanner Appliance
ネットワーク全体のリモートスキャン - ホストとアプリケーション

クラウドエージェント
継続的なセキュリティビューとプラットフォームにより、セキュリティを強化

AWSクラウドコネクタ
クラウドインスタンスとそのメタデータの同期

インターネットスキャナ
エッジに面した IP と URL のペリメータスキャン

Webアプリケーションファイアウォール
侵入を積極的に防御し、アプリケーションを保護

前提条件

これらのオプションは、Qualys ユーザ アカウントで有効にする必要があります。

- Qualys アプリケーション:脆弱性管理(VM/VMDR)、ポリシーコンプライアンス(PC)またはセキュリティ構成評価(SCA)、クラウドエージェント(CA)、Web アプリケーションスキャン(WAS)、Web アプリケーションファイアウォール(WAF)。
- Qualys Amazon AWS EC2 スキャン オプションをオンにする必要があります。利用できない場合は、Qualys 営業担当者 (TAM) またはサポートにお問い合わせください。
- Qualys センサー:仮想 Scanner Appliance、Cloud Agents(必要に応じて)
- マネージャまたはユニットマネージャの役割

始めるのは簡単です

Qualys Cloud Suite、その機能、およびユーザーインターフェイスについては、すでにご存じかもしれません。Qualys を初めて使用する場合は、これらの概要チュートリアルをお勧めします。数分で完了します。

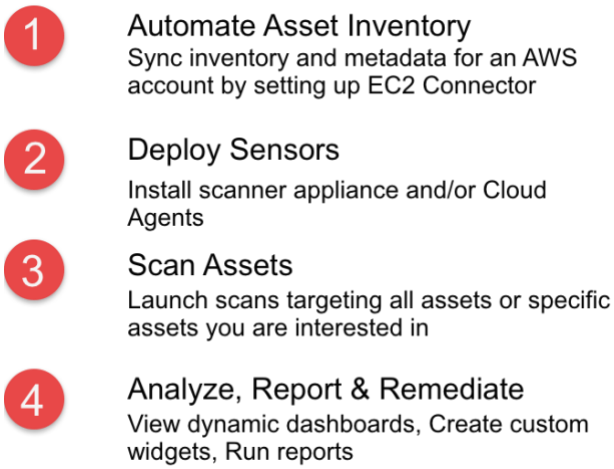
ビデオチュートリアルで 基本を学ぶ

Vulnerability Management Detection and Response. (3 mins)

Policy Compliance Overview

クイックステップ:AWS の保護

Qualys を使用して AWS EC2 を保護するためのユーザーフローを次に示します。



役立つリソース 必要な情報を常に最新の状態に保ちます

コミュニティより

Qualys Training | Free self paced classes, video series, online classes

Qualys Documentation | Getting started guides, quick references, API docs

Qualys AWS EC2 Video Series | Learn how to discover and secure AWS assets

アセットインベントリの自動化

Amazon 用のコネクタは、Amazon API インテグレーションを利用して、Amazon EC2 及び VPC アセットを継続的に検出します。コネクタは、1 つ以上の Amazon アカウントと接続する事で、すべての Amazon EC2 リージョンと Amazon VPC から仮想マシンインスタンスを自動的に検出し、インベントリへの変更を自動的に同期します。

AWS インスタンスは、IP アドレスが時間の経過とともに変化しても、Qualys 内の Amazon インスタンス ID によって追跡されます。Qualys 全体のポリシーとレポートを駆動または影響を与えることができるアセットタグは、インポートプロセスの一部としてアセットエントリに自動的に割り当てられる場合があります。Amazon インスタンスに関する属性とコンテキストメタデータもキャプチャされ、Qualys 内でさらに動的アセットタグ付けを実行するためのデータポイントとして利用できます。

EC2 インスタンスの場合、IP アドレス、タグ、プライベート DNS 名、EC2 インスタンス ID が表示されます。

コネクタのセットアップ

これは、AWS インフラストラクチャを保護するための最初のステップです。このセクションでは、コネクタのセットアップに必要な手順について説明します。Qualys では、AWS アカウントごとに 1 つのコネクタを設定することをお勧めします。Qualys は、4 時間ごとにアセットインベントリを検出して同期します。アセットインベントリはスキャンとは無関係です。

AWS アカウントのコネクタを設定する方法については、「コネクタのオンラインヘルプ」を参照してください。

既存のコネクタとコネクタ アプリのマージ

AssetViewまたはTotalCloudを使用して作成された既存のコネクタを、一元化されたコネクタアプリケーション(アプリ)とマージできるようになりました。新しいコネクタは、AssetView/TotalCloudアプリではなく、コネクタアプリを使用して作成されます。既存のコネクタをマージして、アセットのセキュリティ保護を続行することをお勧めします。

既存のコネクタをマージするには、AWS コネクタの設定の指示に従ってください。

基本アカウント認証の使用

クロスアカウントロールを持つ AWS コネクタは、Qualys アカウントを使用します。Qualys アカウントを使用しない場合は、ベースアカウントを使用して AWS コネクタを設定できます。

自分の AWS アカウントをベースアカウントとして使用するように設定して、 Qualys アカウントを使用する代わりに AWS コネクタを使用します。AWS アカウント ID (複数の AWS アカウントの場合は、少なくとも 1 つの AWS アカウント) を、作成したベースアカウントにマッピングする必要があります。

たとえば、A1、A2、A3 の 3 つの AWS アカウントがあるとします。3 つのアカウントはすべてグローバル リージョンに属しています。グローバルリージョンのベースアカウントを作成する場合、A1、A2、A3 アカウントに関連付けられているすべてのコネクタは、基本アカウントを使用します。

ベースアカウントの作成

新しいコネクタを作成する前に、同じアカウントの種類 (リージョン) の基本アカウントを作成します。基本アカウントがなくてもコネクタを作成できます。コネクタにベースアカウントを使用する場合は、AWS コンソールで設定する必要がある特定の前提条件と設定があります。基本アカウントを設定するために AWS コンソールで必要な詳細な手順と構成を以下に示します。

AWS で IAM ユーザーを作成し、ポリシーを関連付ける

1) **AWS>IAM>Policies>Create Policy** に移動して AssumeRolePolicy を作成します 。

2)JSON タブをクリックし、以下のポリシーを貼り付けます。

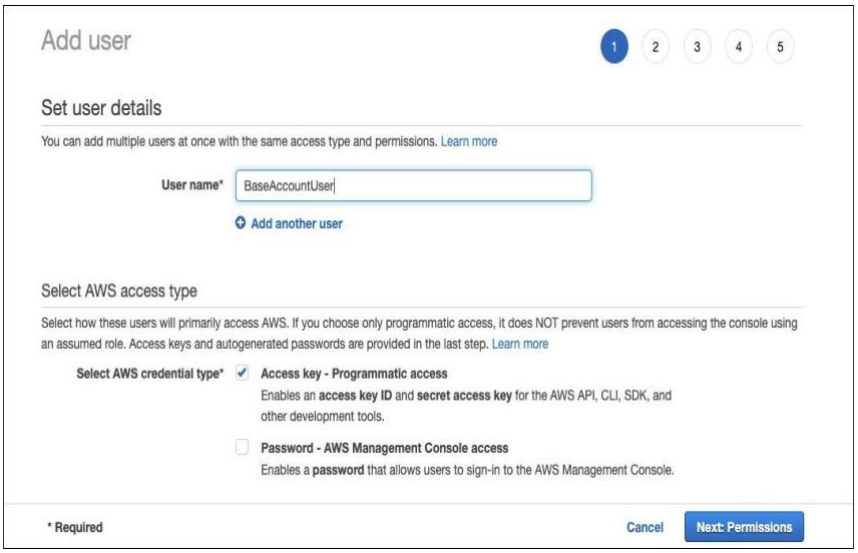
```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "sts:AssumeRole",
        "Resource": "*"
    }
}
```


3) [Next: Tags (次へ: タグ)] > [Next: Review (次へ: レビュー)] をクリックします。

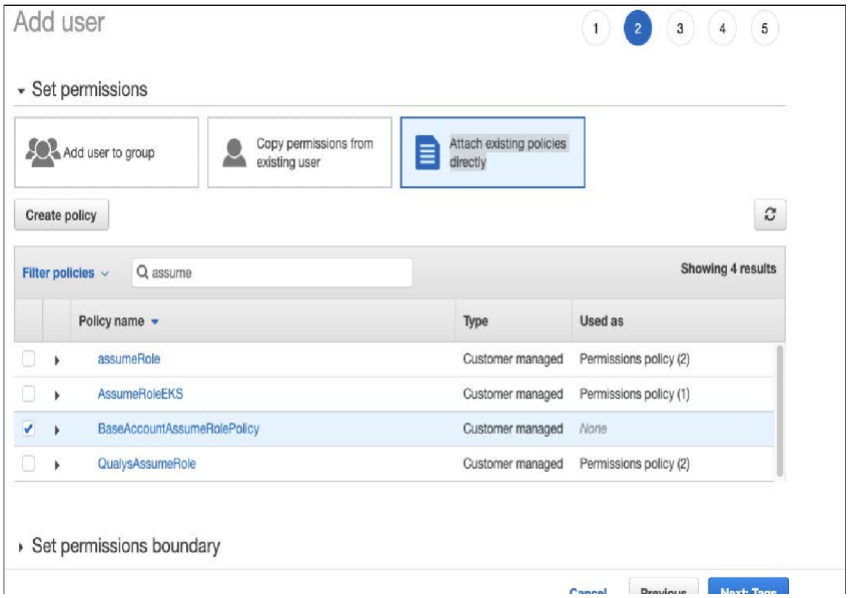
4) ポリシーの名前と説明を追加し、「ポリシーの作成」をクリックします。

5) IAM ユーザーを作成し、AWS > IAM > Users に移動して、[Add user] をクリックします。

6) ユーザー名を指定し、ユーザーのプログラムによるアクセスを有効にします。[Next: Permissions] をクリックします。



7) [アクセス許可の設定] で、 [既存のポリシーを直接アタッチする] に移動します。



8) 手順 1-4 で作成したポリシー名を検索します。

9) [Next:Tags] > Next:Review > Create user をクリックします。

10) 後で使用するために、アクセスキーIDとシークレットアクセスキーをコピーします。[閉じる] をクリックします。

コネクタ・アプリケーションでの基本アカウント構成

1) Qualys コンソールで、[Connectors Application] > [Amazon Web Services Connectors > Base Account] に移動します。

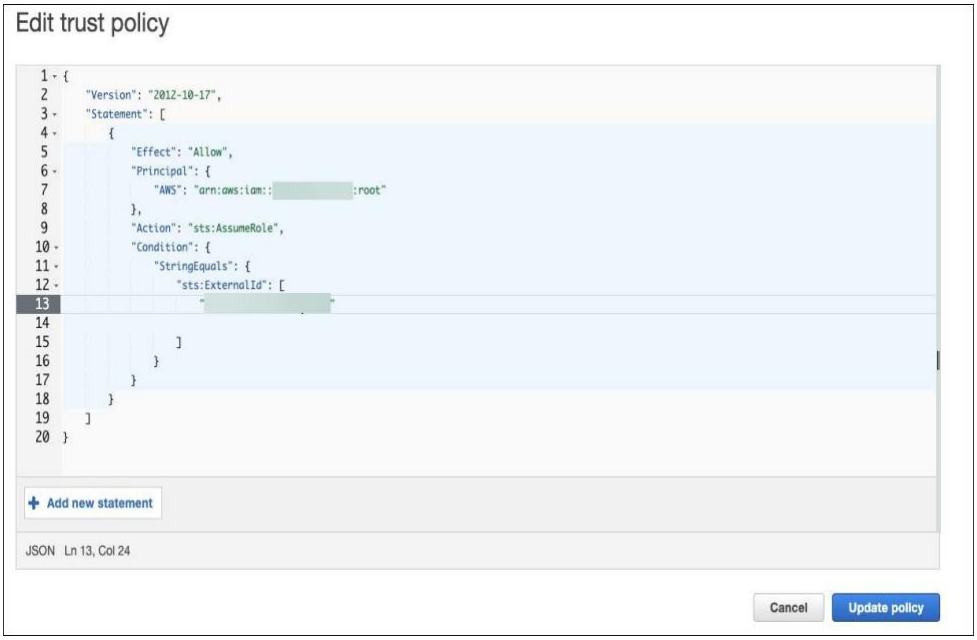
2) AWS 設定の一部として作成されたユーザーの [Access Key Id] と [Secret access key] を貼り付けて、[Save] をクリックします。

既存のコネクタへのカスタムベースアカウントの使用

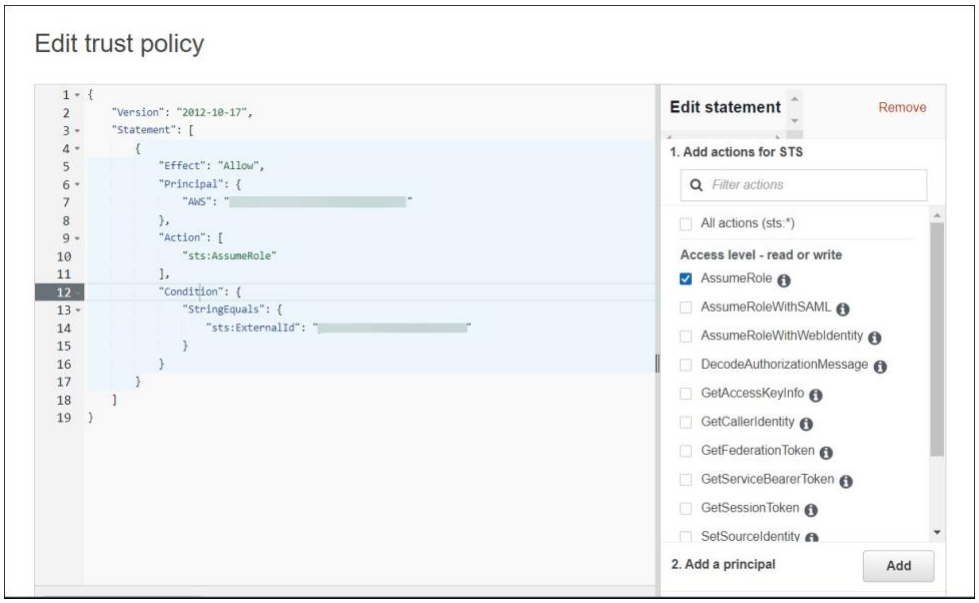
クロスアカウントロールを持つ既存の AWS コネクタをベースアカウントの使用に更新するには、「カスタムベースアカウントの作成」の一部として説明した手順を使用してベースアカウントを作成する必要があります。

1) [AWS > IAM > ロール] に移動し>コネクタロールを選択します。

2) 概要ページで、 [信頼関係] > [信頼ポリシーの編集] を選択します。



4)カスタム基本アカウントを使用するようにプリンシパルを更新します。



5) 「ポリシーの更新」をクリックします。

コネクタはどのように機能しますか?

アセット検出: コネクタは、継続的な同期メカニズムを使用して、クラウドのアセット検出を実行します。コネクタは 4 時間ごとに AWS アカウントと同期し、すべてのインスタンス (終了したインスタンスを含む) をプルします。

AWS は、終了したインスタンスを約 1 時間保持します。ただし、Qualys は終了したすべてのインスタンスの記録を保存し、終了したすべてのインスタンスの履歴と詳細をいつでも追跡できます。

アセットの同期:アセットを Qualys アカウントに追加します。エラーのあるアセット (そのようなアセットがドロップオフされるため) を除き、他のすべてのアセットは Qualys アカウントに追加されます。

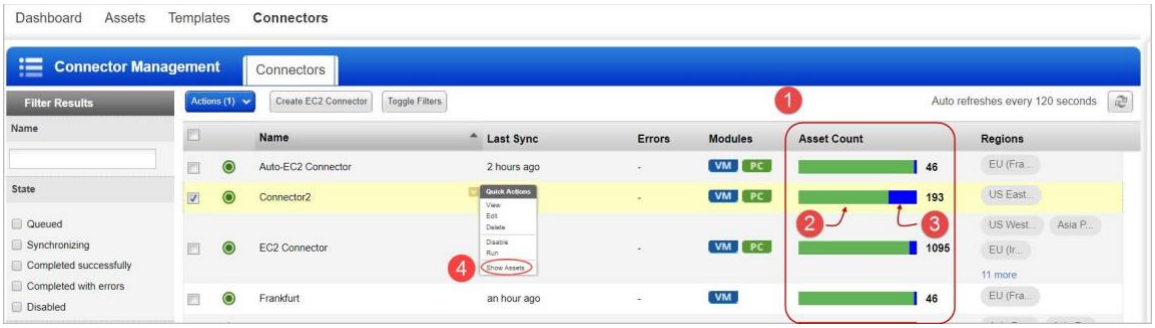
アクティベーション:Scanner Appliance を使用してスキャンを実行する場合は、脆弱性管理/ポリシーコンプライアンス/セキュリティ設定を有効にする必要があります

Qualys アカウントに追加したアセットの評価ライセンス。アセットを手動でアクティブ化することも、コネクタのセットアップ中に自動アクティブ化を有効にすることもできます。

アクティベーションから除外: アクティベーションから除外される終了したインスタンスとは別に、m1.small、t1.micro、t2.nano、または t3.nano インスタンスもアクティベー

ションから除外されます。テクニカル アカウント マネージャーまたは Qualys サポートに連絡して、この制限を解除し、コネクタ設定に基づいてこれらのインスタンス タイプのアセットを自動アクティブ化できるようにしてください。有効にすると、このようなインスタンスに対してクラウドペリメータスキャンを開始できます。または、このようなインスタンスで Cloud Agent を使用することもできます。

インポートされたアセットの表示



コネクタの作成が完了すると、コネクタはインスタンスのプルを開始します。コネクタの実行が完了した後に表示されるさまざまな情報を確認しましょう。

1. **アセット数** - アセット数列には、最新のコネクタ実行で検出および同期されたアセットが表示されます。

2. **同期されたアセット** - 「アセット数」列の緑色の部分は、同期されたアセットを表します。同期された数は、Qualys で正常に処理されたアセットを表します。

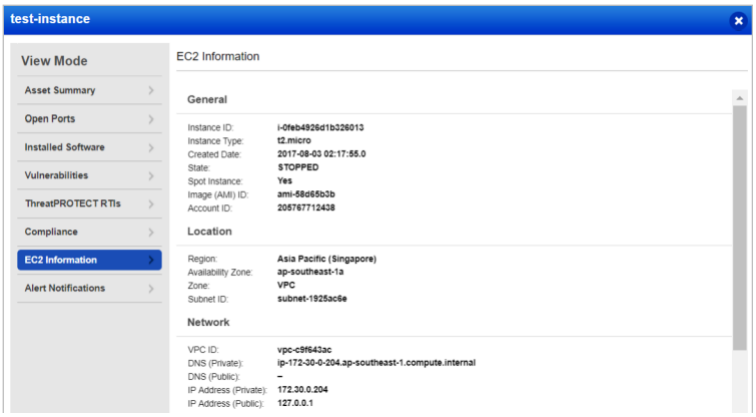
3. **除外されたアセット** - 青色の部分は、同期されているが、VM/PC/SCA のアクティブ化から除外されているアセットを表します。除外されるアセットは、Qualys スキャナーでスキャンできない終了インスタンス、または m1.small、t1.micro、t2.nano、t3.nano です。テクニカルアカウントマネージャーまたは Qualys サポートに連絡して、この制限を解除し、コネクタ設定に基づいてこれらのインスタンスタイプのアセットを自動アクティブ化できるようにしてください。アクティブ化すると、クラウドを起動できます

このようなインスタンス(m1.small、t1.micro、t2.nano、または t3.nano)のペリメータスキャン。除外されたアセットは、同期されたアセットのサブセットです。

4. **アセットの表示** – 一定期間にコネクタによって検出されたアセットの合計数。

エラーのあるアセット - アセット数列には、エラーのあるアセットを表す赤色の部分も表示される場合があります。エラーのあるアセットは、Qualys での処理中に問題が発生したアセットです。

コネクタによって収集されたアセットを表示するには、AssetView に移動します。[アセットの詳細] ページの [EC2 情報] タブには、収集された AWS インスタンスのメタデータが表示されます。以下は、収集した情報を表示するサンプルのスクリーンショットです。



EC2 インスタンスが検出されたら、Amazon EC2 インフラストラクチャのスキャンと保護を開始する準備が整います。

AWS メタデータ

このセクションでは、Qualys Cloud Agent、AssetView Connector、および Qualys Scanner によって提供されるクラウドプロバイダーのメタデータについて説明します。

AssetView コネクタと Cloud Agent

全般：

- Reservation ID
- Instance ID
- Instance Type
- Created Date
- Image (AMI) ID
- Account ID
- Instance State (Only Running for QCA data collection)

ロケーション：

- Region
- Availability Zone
- Zone

ネットワーク：

- VPC ID
- DNS (Private)
- DNS (Public)
- Local Hostname
- MAC Address
- Subnet ID
- Security Groups
- Security Groups IDs
- IP Address (Private)
- IP Address (Public)

AssetView コネクタのみ

- AWS Tags
- Instance State Updates (Stopped, Terminated, ...)

QID - 370098 Amazon EC2 Linux インスタンスのメタデータ

1) metadata/

- AMI ID
- AMI Launch Index
- AMI Manifest Path
- Hostname
- Instance Action
- Instance ID
- Instance Type

- Kernel ID
- Local Hostname
- Local Ipv4
- MAC
- Public Hostname
- Public Ipv4
- Reservation ID
- Security Groups
- Ancestor AMI Ids
- Profile

  dynamic/instance-identity/document/

  - accountId
  - availabilityZone
  - kernelId
  - ramdiskId
  - pendingTime
  - architecture
  - privateIp
  - devpayProductCodes
  - version
  - billingProducts
  - instanceId
  - imageId
  - instanceType
  - region

アセットを検出するために EC2 Connector によって使用される AWS API

Qualys は 3 つの API を使用して EC2 インスタンスを検出し、AWS アカウントからそれらのインスタンスに関する追加情報を識別します。これらの API に関する情報は、以下の Amazon AWS Web サイトの場所にあります。

DescribeInstances API

https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_DescribeInstances.html

DescribeImages API

https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_DescribeImages.html

DescribeNetworkInterfaces API

https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_DescribeNetworkInterfa ces.html

ディスカバリ ジョブは、オンデマンドで実行することも、デフォルトの頻度(4 時間ごと)で実行することもできます。現在、この頻度は設定できません。

EC2 コネクタの Qualys API

また、EC2 コネクタの各種操作を API 経由で実行することもできます。AWS に関連する Qualys API の使用の詳細については、『Asset Management and Tagging API v2 User Guide』を参照してください。

便利な EC2 コネクタ API を次に示します。

AWS コネクタの作成

https://qualysapi.qualys.com/qps/rest/3.0/create/am/awsassetdataconnector

コネクタの実行

https://qualysapi.qualys.com/qps/rest/3.0/run/am/assetdataconnector/<id>

Get Host Asset Info (EC2 インスタンスのメタデータの取得)

https://qualysapi.qualys.com/qps/rest/2.0/get/am/hostasset/<id>

AWS EC2 環境でのスキャン

ネットワークの基本でいくつかの用語に慣れ親しんでおきましょう。

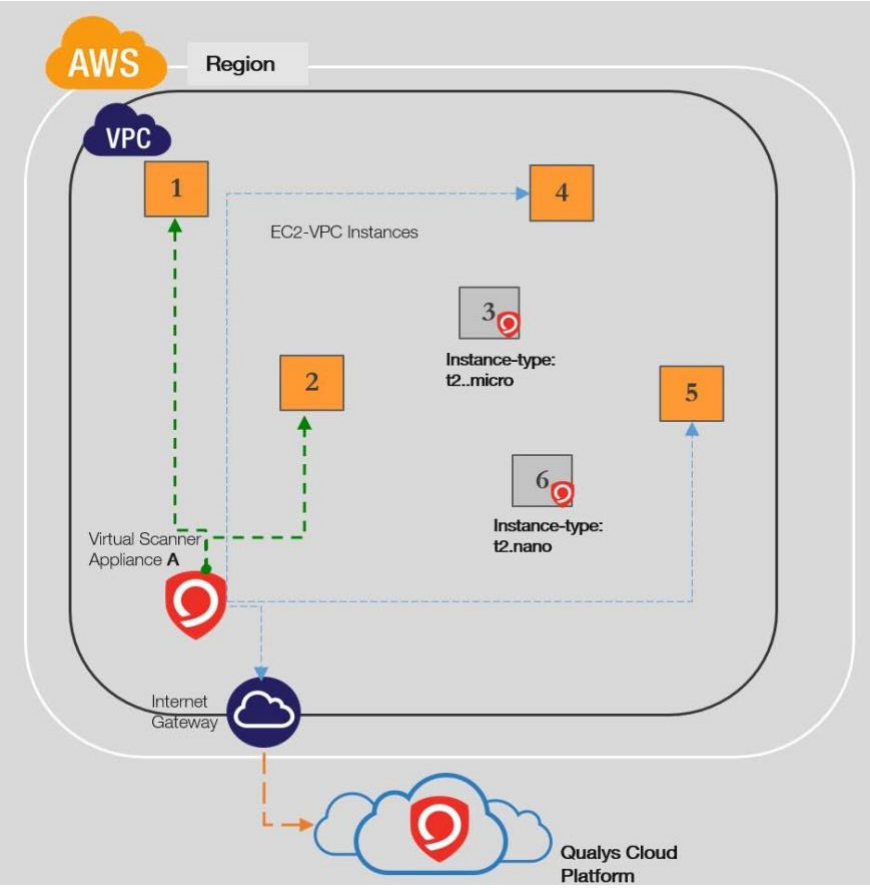
VPC: 定義した仮想ネットワークで AWS リソースを起動できます。これは、自社のデータセンターで運用する従来のネットワークとよく似ており、AWS のスケーラビリティを利用できるという利点があります。

VPC ピアリング: 2 つの VPC 間でトラフィックをルーティングできるネットワーク接続。

トランジットゲートウェイ: 仮想プライベートクラウド (VPC) とオンプレミスネットワークを相互接続するために使用できるネットワークトランジットハブ。

次に、AWS EC2 環境でのスキャンのさまざまなシナリオを見てみましょう。

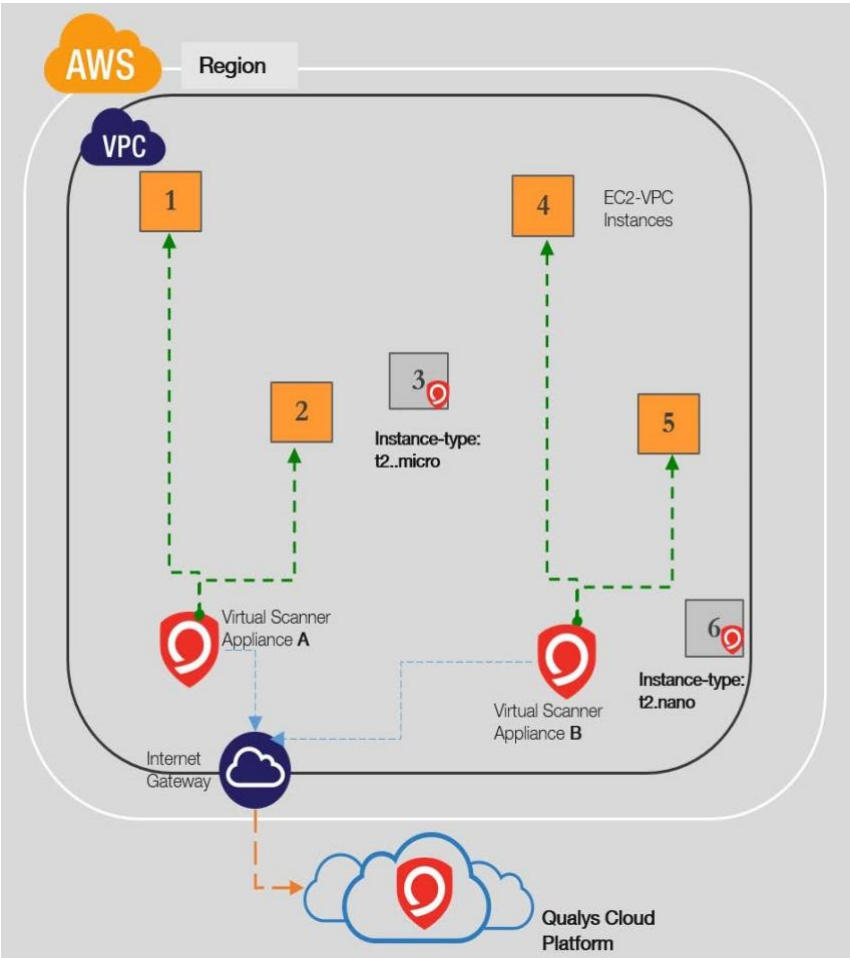
1 つのスキャナーが VPC 内の複数のインスタンスをスキャンする



スキャナは、https (セキュリティ グループとインターネット ゲートウェイ)経由で Qualys Cloud Platform および AWS EC2 および STS エンドポイントと通信するように設定する必要があります。

AWS では、環境への潜在的な中断を最小限に抑えるために、次の EC2 インスタンス タイプ (T3.nano、T2.nano、T1.micro、および M1.small) をセキュリティ評価から除外することをお勧めします。 クラウド エージェントは、それらをスキャンするための推奨される方法です。

複数のスキャナーが VPC 内の複数のインスタンスをスキャンする

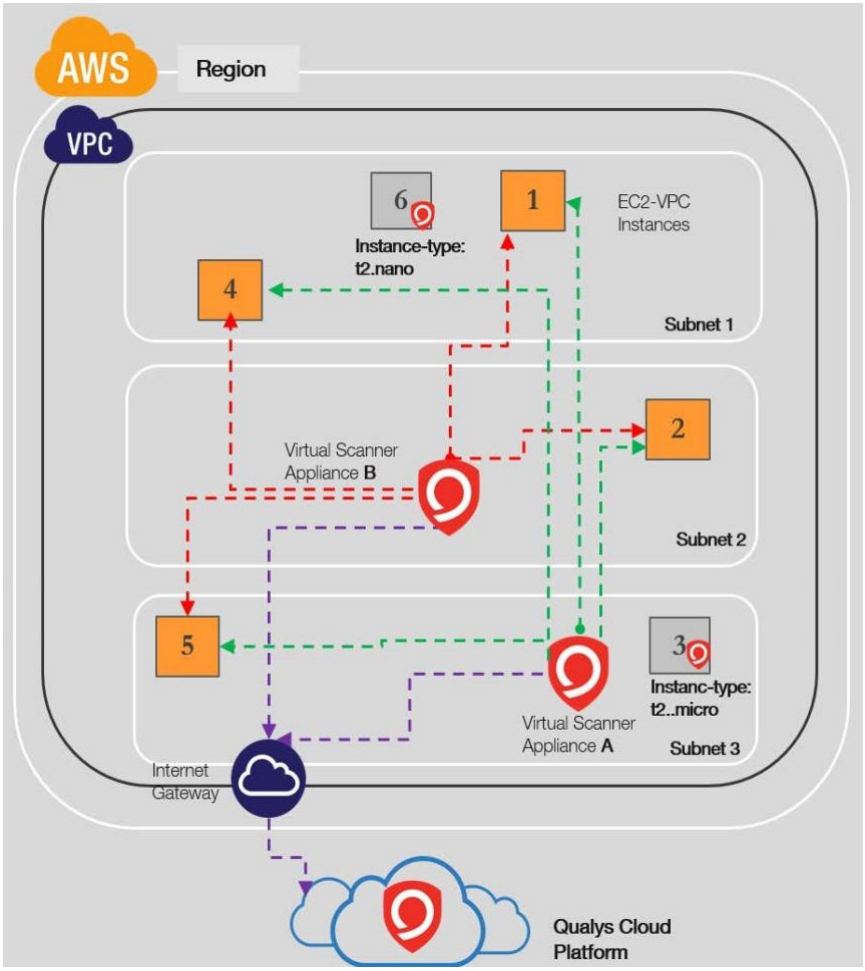


インスタンスの数とスキャン頻度によっては、VPC 内の複数のインスタンスをスキャンするために複数のスキャナーが必要になる場合があります。VPC ごとに少なくとも 1 つのスキャナーが必要です。要件に基づいてさらに追加できます。

スキャナーは、Qualys Cloud Platform および AWS EC2 および STS エンドポイントと (セキュリティ グループとインターネット ゲートウェイを介して) 通信するように設定する必要があります。

AWS では、環境の中断を最小限に抑えるために、セキュリティ評価から次の EC2 インスタンスタイプ (T3.nano、T2.nano、T1.micro、M1.small) を除外することを推奨しています。クラウドエージェントは、それらをスキャンするための推奨される方法です。

1 つのスキャナが VPC 内のサブネット全体で複数のインスタンスをスキャンする



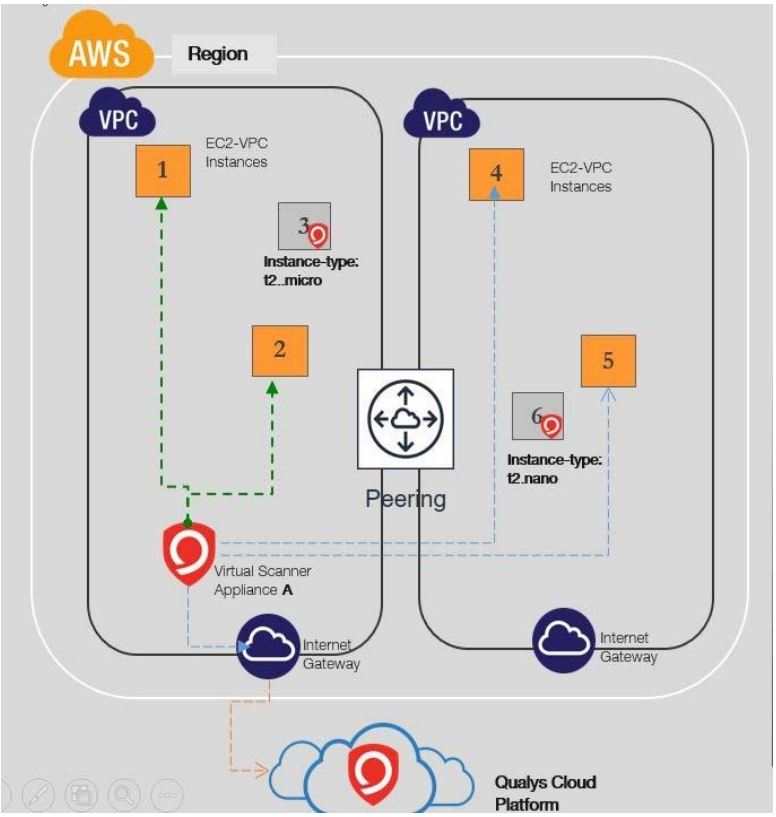
スキャナは、ネットワークに制限が導入されていない限り、通常、VPC 内のサブネット間で動作できます。

スキャナーは、Qualys Cloud Platform および AWS EC2 および STS エンドポイントと https 経由で (セキュリティ グループまたはインターネット ゲートウェイ経由で) 通信するように設定する必要があります。

AWS では、環境の中断を最小限に抑えるために、セキュリティ評価から次の EC2 インスタンスタイプ (T3.nano、T2.nano、T1.micro、M1.small) を除外することを推奨しています。

クラウドエージェントは、それらをスキャンするための推奨される方法です。

1 つのスキャナーが、リージョン内のピアリングされた VPC 間で複数のインスタンスをスキャンする



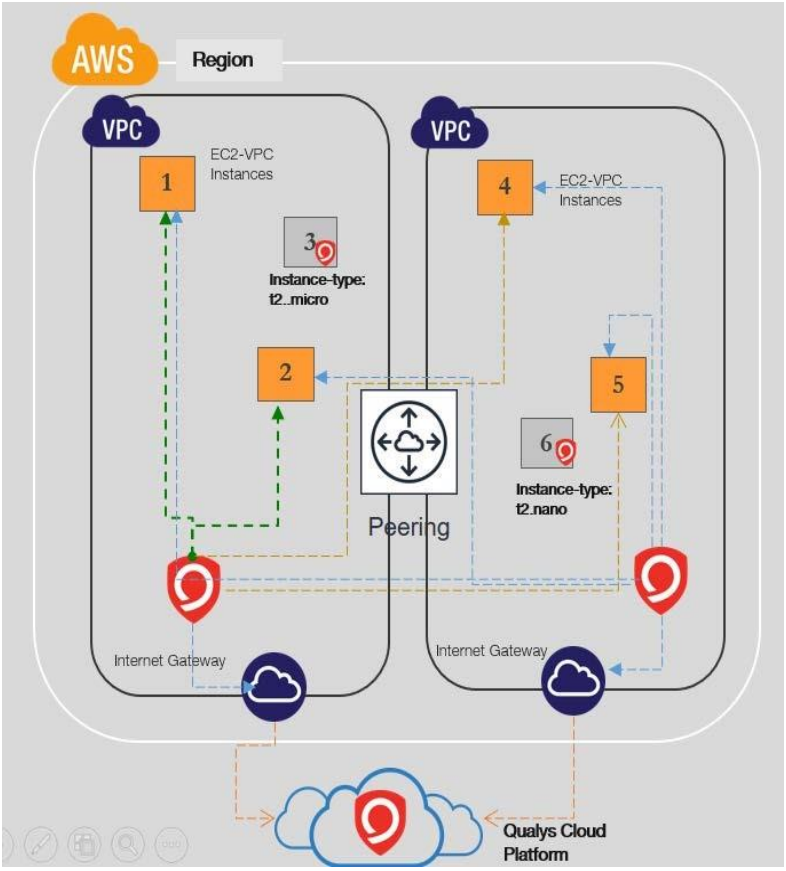
要件に基づいてさらに追加できます。

スキャナーは、Qualys Cloud Platform および AWS EC2 および STS エンドポイントと https 経由で (セキュリティグループとインターネットゲートウェイ経由で)通信するように設定する必要があります。

AWS は、次の EC2 インスタンスタイプ (T3.nano、T2.nano、T1.micro、M1.small) をセキュリティ評価から除外して、環境への潜在的な中断を最小限に抑えます。

クラウドエージェントは、それらをスキャンするための推奨される方法です。

ピアリングされた VPC 間で複数のインスタンスをスキャンするには、複数のスキャナーが必要になる場合がある

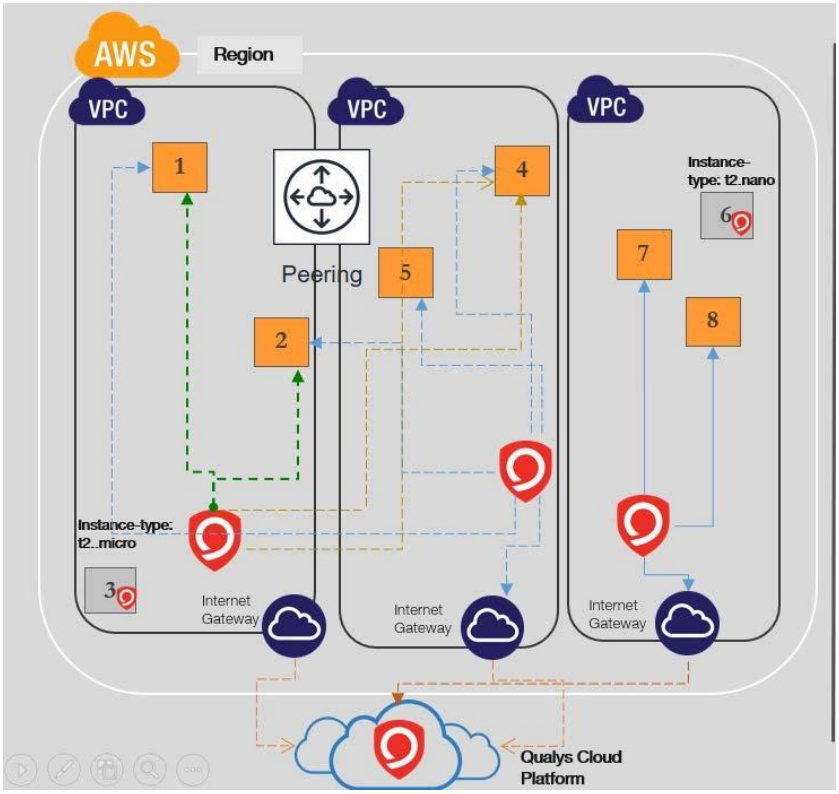


インスタンスの数とスキャン頻度に基づいて、リージョン内のピアリングされた VPC 間で複数のインスタンスをスキャンするには、複数のスキャナーが必要になる場合があります。要件に基づいて、VPC ペリメータを越えたスキャンを許可するためにさらに追加できます。スキャナーは、Qualys Cloud Platform および AWS EC2 および STS エンドポイントと https 経由で (セキュリティ グループとインターネット ゲートウェイ経由で) 通信するように設定する必要があります。

AWS では、環境の中断を最小限に抑えるために、セキュリティ評価から次の EC2 インスタンスタイプ (T3.nano、T2.nano、T1.micro、M1.small) を除外することを推奨しています。

クラウドエージェントは、それらをスキャンするための推奨される方法です。

スキャナーは、ピアリングされていない VPC のインスタンスをスキャンできません



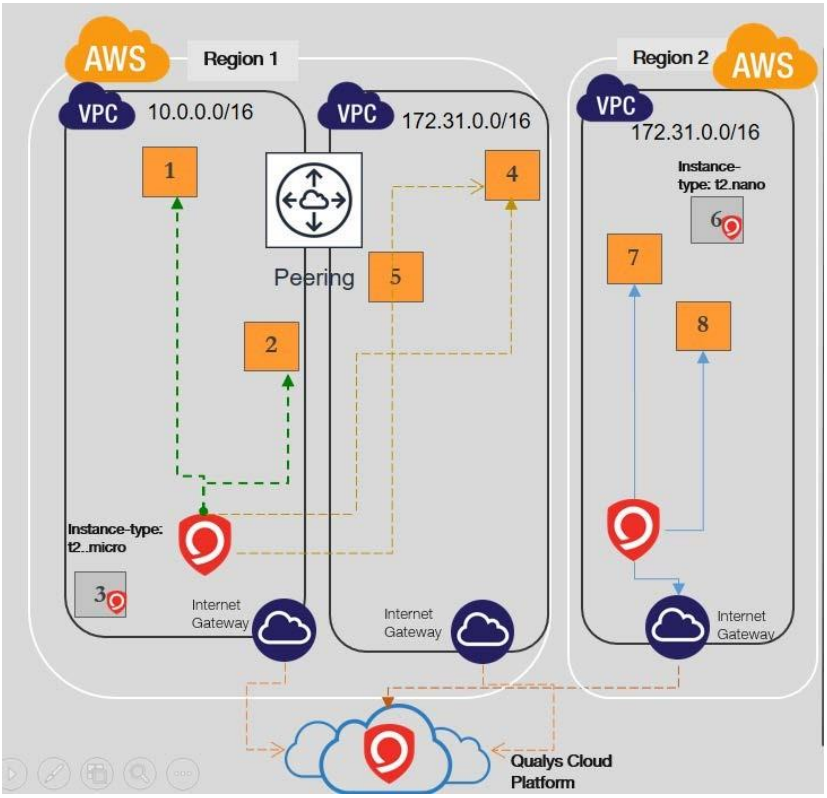
要件に基づいて、VPC ペリメータを越えたスキャンを許可するためにさらに追加できます。

スキャナーは、Qualys Cloud Platform および AWS EC2 および STS エンドポイントと https 経由で (セキュリティ グループとインターネット ゲートウェイ経由で) 通信するように設定する必要があります。

AWS では、環境の中断を最小限に抑えるために、セキュリティ評価から次の EC2 インスタンスタイプ (T3.nano、T2.nano、T1.micro、M1.small) を除外することを推奨しています。

クラウドエージェントは、それらをスキャンするための推奨される方法です。

スキャナーは、IP アドレスが重複している VPC のインスタンスをスキャンできません



1 つのスキャナでは、1 つのサブネットに到達できるため、IP アドレスが重複する VPC 内のインスタンスをスキャンできません。要件に基づいて、VPC ペリメータを越えたスキャンを許可するためにさらに追加できます。

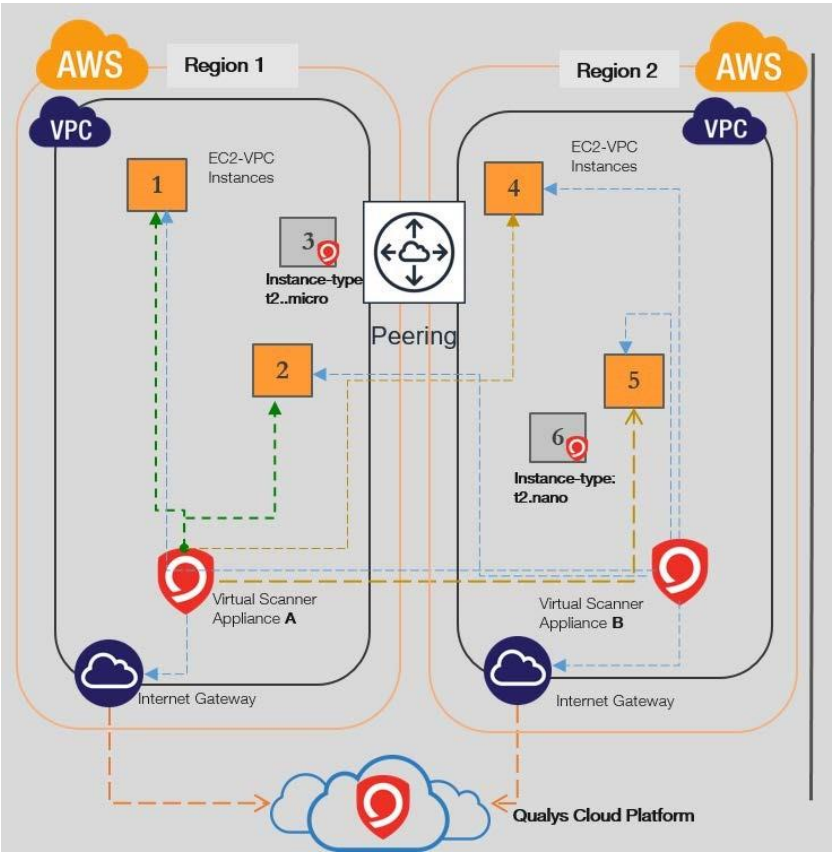
注: VPC ピアリングは VPC A と C の間で設定できますが、B と C の間でサブネットが重複しているため、スキャナーはルート テーブルに基づいてそのうちの 1 つにしか到達しません。

スキャナーは、Qualys Cloud Platform および AWS EC2 および STS エンドポイントと https 経由で (セキュリティ グループとインターネット ゲートウェイ経由で) 通信するように設定する必要があります。

AWS では、環境の中断を最小限に抑えるために、セキュリティ評価から次の EC2 インスタンスタイプ (T3.nano、T2.nano、T1.micro、M1.small) を除外することを推奨しています。

クラウドエージェントは、それらをスキャンするための推奨される方法です。

1 つのスキャナーで、異なるリージョンのピアリングされた VPC 間で複数のインスタンスをスキャンします



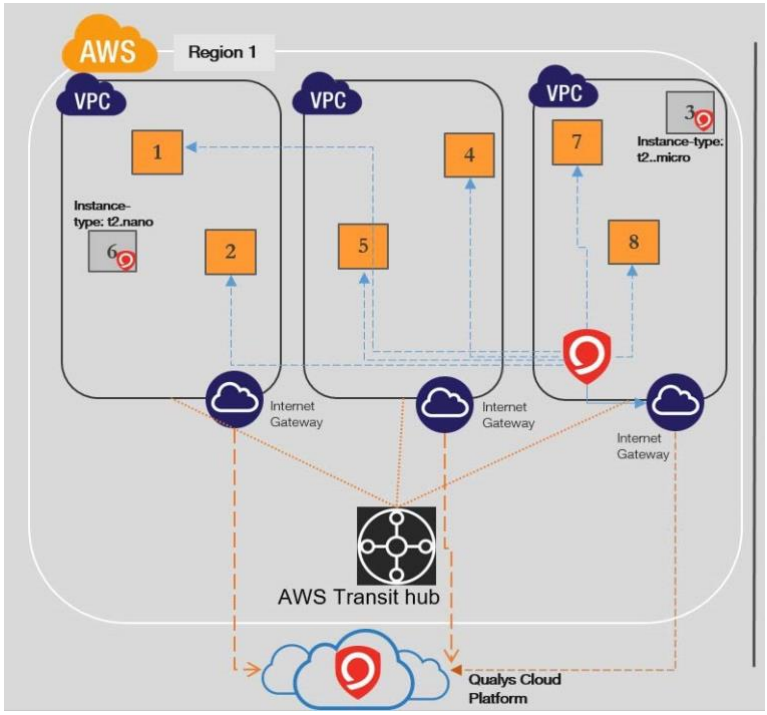
要件に基づいて、VPC ペリメータを越えたスキャンを許可するためにさらに追加できます。

スキャナーは、Qualys Cloud Platform および AWS EC2 および STS エンドポイントと https 経由で (セキュリティグループとインターネット ゲートウェイ経由で) 通信するように設定する必要があります。

AWS では、環境の中断を最小限に抑えるために、セキュリティ評価から次の EC2 インスタンスタイプ (T3.nano、T2.nano、T1.micro、M1.small) を除外することを推奨しています。

クラウドエージェントは、それらをスキャンするための推奨される方法です。

1 つのスキャナーは、トランジットで接続されたリージョン内の VPC 間で複数のインスタンスをスキャンします



ネットワークトランジットハブは仮想プライベートクラウド(VPC)間の相互接続を可能にするため、1 つのスキャナーを使用して、トランジットゲートウェイで接続されたリージョン内の VPC 間で複数のインスタンスをスキャンできます。

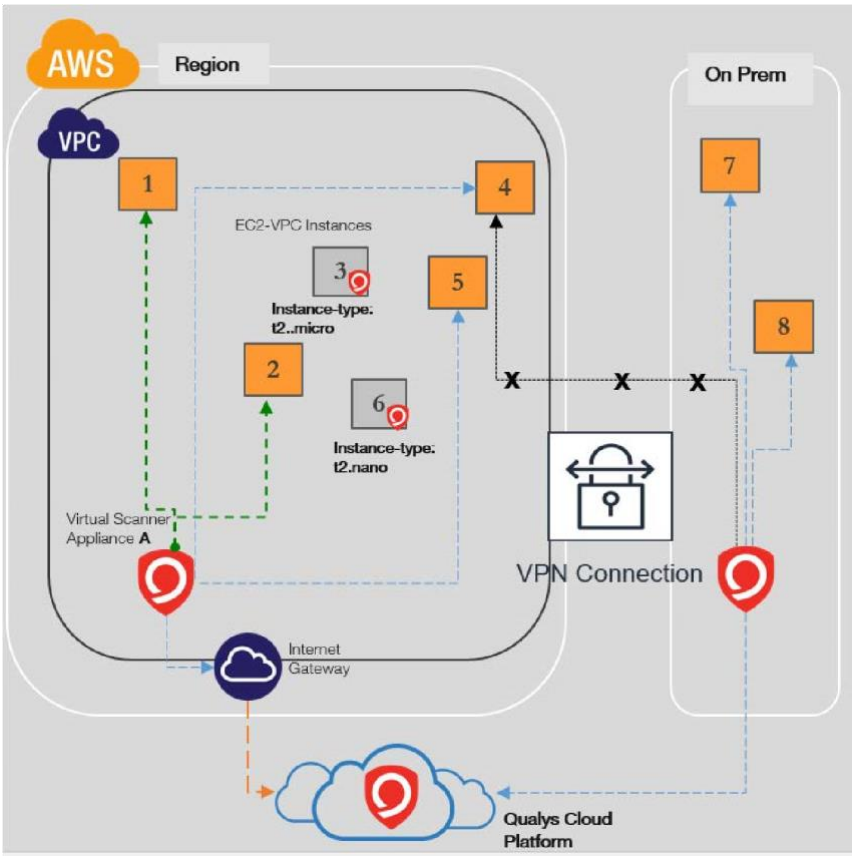
スキャナは、Qualys Cloud と通信するように設定する必要があります

プラットフォームと AWS EC2 & STS エンドポイントを https 経由で(セキュリティ グループとインターネット ゲートウェイ経由で) 通信するように設定する必要があります。

AWS では、環境の中断を最小限に抑えるために、セキュリティ評価から次の EC2 インスタンスタイプ (T3.nano、T2.nano、T1.micro、M1.small) を除外することを推奨しています。

クラウドエージェントは、それらをスキャンするための推奨される方法です。

オンプレミス・スキャナーはクラウド・インスタンスのスキャンには推奨されません



スキャナーは、Qualys Cloud Platform および AWS EC2 および STS エンドポイントと https 経由で (セキュリティ グループとインターネット ゲートウェイ経由で) 通信するように設定する必要があります。

オンプレミスネットワーク上にあるスキャナーは、クラウド対応ではなく、従来のスキャンワークフローを使用しているため、クラウドインスタンスのスキャンには使用しないでください。

t2.micro と t2.nano のインスタンスタイプは、AWS ペネトレーションテストルールに従ってスキャンされません。

クラウドエージェントは、それらをスキャンするための推奨される方法です。

センサーの展開

Qualys Cloud Platform のコアサービスである Qualys センサーは、グローバル企業全体にセキュリティを簡単に拡張できるようにします。これらのセンサーは、リモートで展開でき、一元管理され、自己更新可能です。データを収集し、Qualys Cloud Platform に自動的に送信し、Qualys Cloud Platform は、脅威の特定と脆弱性の排除を支援するために、情報を継続的に分析して関連付けるコンピューティング能力を備えています。AWS の場合、センサーは AMI および軽量エージェントの形式で仮想アプライアンスとして提供されます。

スキャンの前に、センサーを展開する必要があります。好みに応じて、仮想 Scanner Appliance または Qualys Cloud Agent を導入できます。では、これらのセンサーの導入手順を見ていきましょう。

Deploying Virtual Scanner Appliance

Deploying Qualys Cloud Agent

Virtual Scanner Appliance の導入

仮想スキャナーの展開に関連する実際の手順を実行する前に、ライセンス/コストの側面と展開の推奨事項を理解しましょう。

コストとライセンス

Qualys Virtual Scanner Appliance は、AWS Marketplace で Amazon マシンイメージ (AMI) として入手でき、Amazon EC2-Classic および EC2-VPC で起動する準備ができています。

次の 2 つの点を考慮する必要があります。

- 仮想スキャナ ライセンス サブスクリプションの Qualys コスト
- アプライアンスを EC2 インスタンスとして実行するためのコンピューティングリソースの AWS コスト

Qualys コスト

実行する仮想 Scanner Appliance インスタンスごとに Qualys ライセンスを取得する必要があります。このライセンスは AWS からではなく Qualys から取得され、当社の Scanner Appliance は BYOL(つまり、「Bring Your Own License」)モデルで AWS Marketplace にリストされています。Qualys Cloud Platform UI で定義する各 Qualys 仮想 Scanner Appliance プロファイルは、1 つの仮想 Scanner Appliance ライセンスを消費します。Qualys サブスクリプション

から仮想 Scanner Appliance プロファイルを削除すると、そのライセンスは解放され、すぐに再利用できるようになります。

Qualys テクニカル アカウント マネージャーまたは Qualys リセラーに連絡して、価格の見積もりまたは評価を依頼してください。

AWS Cost

各仮想 Scanner Appliance インスタンスは、独自の AWS アカウントの 1 つで起動されます。アプライアンスの実行コストを AWS に支払う責任があります。

これらのコストには、次のものが含まれます。

2) インスタンスの種類に基づくコンピューティング容量

3) ストレージ

4) データ転送　IN/OUT

コンピューティング容量の料金 (CPU、RAM) は、インスタンスを実行するためのコストの圧倒的に最大の部分です。Scanner Appliance を常に実行し続ける必要はありません。インスタンスが停止している時間帯には、プロビジョニングされたストレージ料金が GB 単位でのみ発生します。ただし、スキャナーは、ソフトウェアと署名を最新の状態に保つために、少なくとも週に数時間オンにする必要があります。

スキャナーのデプロイに関する推奨事項

次に、ネットワークトポロジと Scanner Appliance をホストするための EC2 インスタンスのサイズに基づいてスキャナを導入するための Qualys の推奨事項を示します。

スキャナーをホストするためのインスタンスサイズ

Qualys Virtual Scanner Appliance をホストするために、Qualys でスキャナインスタンスでサポートされる最大サイズは 8 CPU と 16 GB RAM です。また、A1、c6g、m6g、t4g、r6g インスタンスファミリーなどの ARM ベースのアーキテクチャインスタンスタイプでのスキャナーデプロイはサポートされていません。スキャンされる EC2 インスタンスの数とインスタンスがスキャンされる回数に基づいて、最大 8 つの CPU と 16 GB の RAM にスケールアップできます。

スキャン容量に基づいてインスタンスタイプを選択するには (2.7.45 までのバージョンにのみ適用可能)、 https://success.qualys.com/discussions/s/article/000006880.

様々なスキャンジョブに必要な Scanner Appliance の容量の詳細については、https://success.qualys.com/support/s/article/000003491.

ENA インスタンスのサポート

Qualys Virtual Scanner Appliance は、拡張ネットワーキング(ENA)および NVMe SSD ボリュームをサポートするインスタンスタイプにも導入できます。現在の世代のインスタンスタイプで AWS がサポートするネットワークおよびストレージ機能については、次の表を参照してください。

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-types.html#instancetype-summary-table

Qualys Virtual Scanner Appliance は、最大 16 個の CPU と 16 GB の RAM を持つインスタンスタイプにのみデプロイできます。

スキャン対象の制限

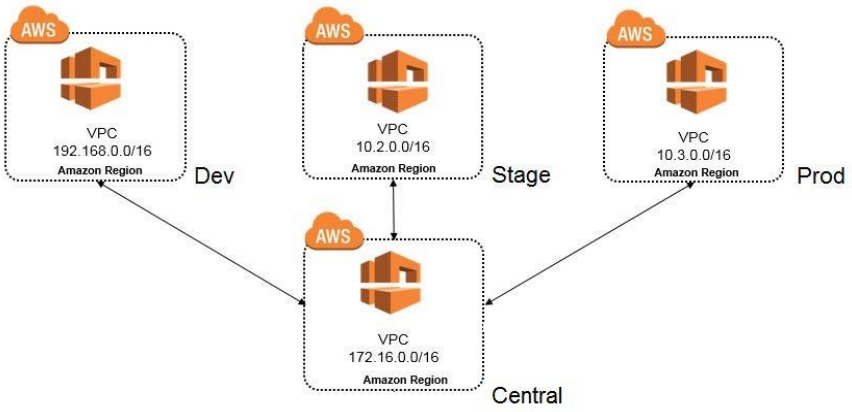
t1.micro、m1.small、t2.nano インスタンスタイプを使用するターゲットでは、スキャンを起動できません。

ネットワークトポロジーに基づくスキャナーの配置

Amazon Virtual Private Cloud (Amazon VPC) は、AWS クラウド上でネットワークを設計および実装するための多くのオプションを AWS のお客様に提供するための包括的な仮想ネットワーク機能セットを提供します。Amazon VPC を使用すると、お客様は論理的に分離された仮想ネットワークをプロビジョニングして、AWS リソースをホストできます。AWS ネットワークの設定方法に基づいて、スキャナーの配置方法に関する推奨事項をいくつか紹介します。

5) リージョン内の非ピアリング VPC - VPC がピアリングされていない場合、Qualys では、VPC ごとに 1 つ以上のスキャナをリージョンごとに持つことを推奨しています。

6) リージョン内のピアリングされた VPC - リージョン内の他の VPC にピアリングされた中央 VPC に 1 つ以上のスキャナーを配置できます (ハブ 'n' スポーク モデル)。以下はその例です。



7) リージョン間の VPC - VPN または VPC トランジットを持つ VPC に 1 つ以上のスキャナーを配置できます。

インスタンスのスナップショット/クローニングは許可されていません

仮想スキャナインスタンスのスナップショットまたはクローンを使用して新しいインスタンスを作成することは固く禁じられています。新しいインスタンスはスキャナーとして機能しません。すべての構成設定とプラットフォーム登録情報が失われます。これにより、スキャンが失敗し、元のスキャナーでエラーが発生する可能性もあります。

インスタンスの移動/エクスポートは許可されていません。

登録済みのスキャナーインスタンスを仮想化プラットフォーム(HyperV、VMware、XenServer)から任意のファイル形式で AWS クラウドプラットフォームに移動またはエクスポートすることは固く禁じられています。

これにより、スキャナーの機能が壊れ、スキャナーはすべての設定を永久に失います。

何が必要ですか?

アカウントで [仮想スキャナー] オプションをオンにする必要があります。このオプションを有効にしたい場合は、Qualys サポートまたはテクニカル アカウント マネージャにお問い合わせください。

マネージャまたは「仮想 Scanner Appliance の管理」権限を持つサブユーザである必要があります。この権限は、ユニットマネージャに付与できます。サブスクリプションは、このアクセス許可をスキャナーに付与できるように構成されている場合があります。

スキャナーの展開

スキャナーのデプロイには、Qualys と AWS での設定が含まれます。

考慮すべき点がいくつかあります...

次の機能はサポートされておらず、すべてのクラウド(プライベートおよびパブリック)プラットフォームで無効になっています。

8) WAN/スプリットネットワーク設定 - スプリットネットワーク設定の「WAN インターフェイス」オプションは、スキャナーUI/コンソールからは使用できません。Cloud UI からの LAN/単一ネットワーク設定のみをサポートし、スキャンと Qualys サーバへの接続の両方に使用されます。

9) NATIVE VLAN:ネイティブ VLAN を設定するための「VLAN on LAN」オプションは、スキャナーUI/コンソールからは使用できません。

10) スタティック VLAN(IPV4 および IPV6):スタティック VLAN を設定するための「VLAN」オプションは、Qualys UI からは使用できません。

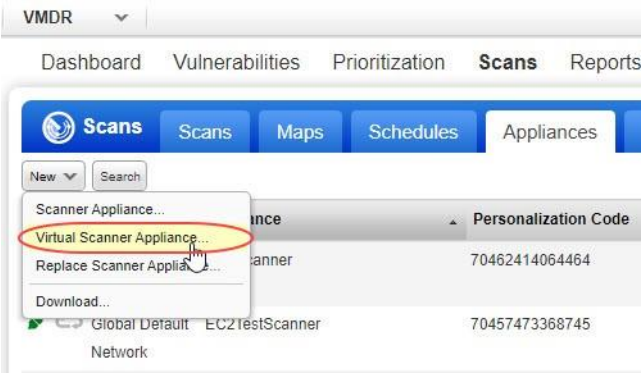
11) スタティック ルート(IPV4 および IPV6):「スタティック ルート」を設定するオプションは、Qualys UI からは使用できません。

12) IPV6 ON LAN:「IPv6 on LAN」を設定するオプションは、Qualys UI からは使用できません。

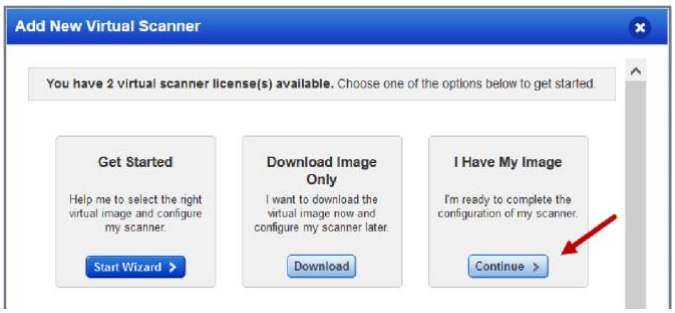
Qualys での設定

仮想アプライアンスの設定 - パーソナライゼーションコードの取得

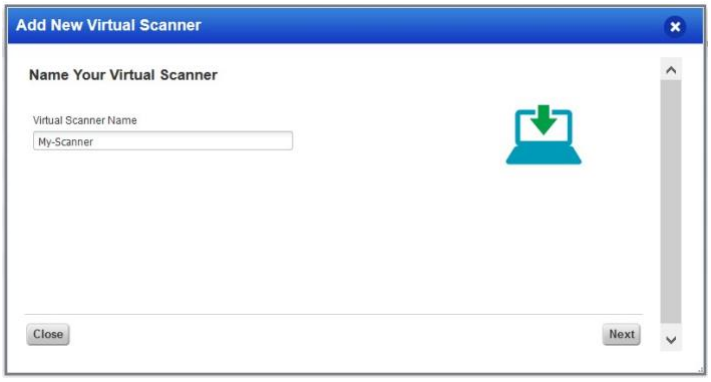
Qualys アプリ ピッカーから [VM/VMDR] または [PC] を選択します。次に、[Scans > Appliances] に移動し、[New > Virtual Scanner Appliance] を選択します。



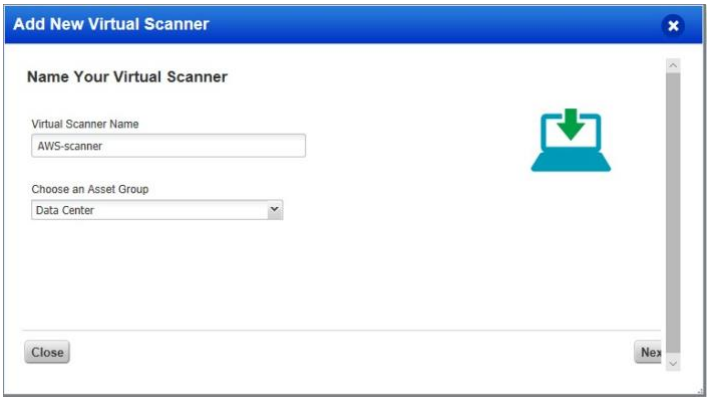
「I have My Image」を選択し、「Continue」をクリックします。



名前を入力し、「次へ」をクリックします。

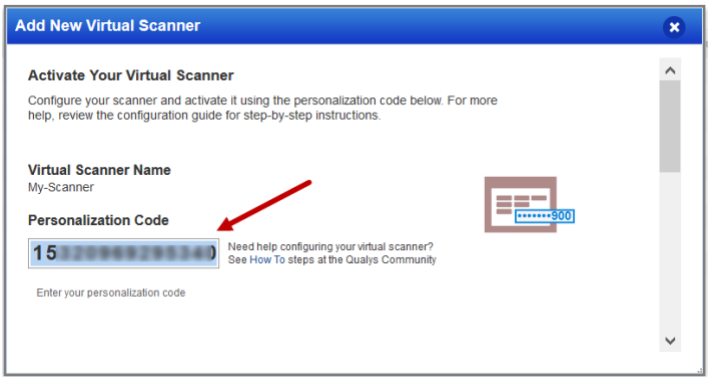


サブユーザーの場合は、マネージャーユーザーによってビジネスユニットに割り当てられたアセットグループを選択する必要があります。アセット グループが表示されない場合マネージャーに依頼して、ビジネスユニットにアセットグループ([すべて]グループ以外)を割り当ててください。



画面の指示に従って、仮想スキャナーを構成します。「次へ」をクリックします。

個人用設定コードを取得します。これは、AMI インスタンスを起動するために必要になります。



AWS での設定

Amazon AWS で AMI インスタンスを起動する

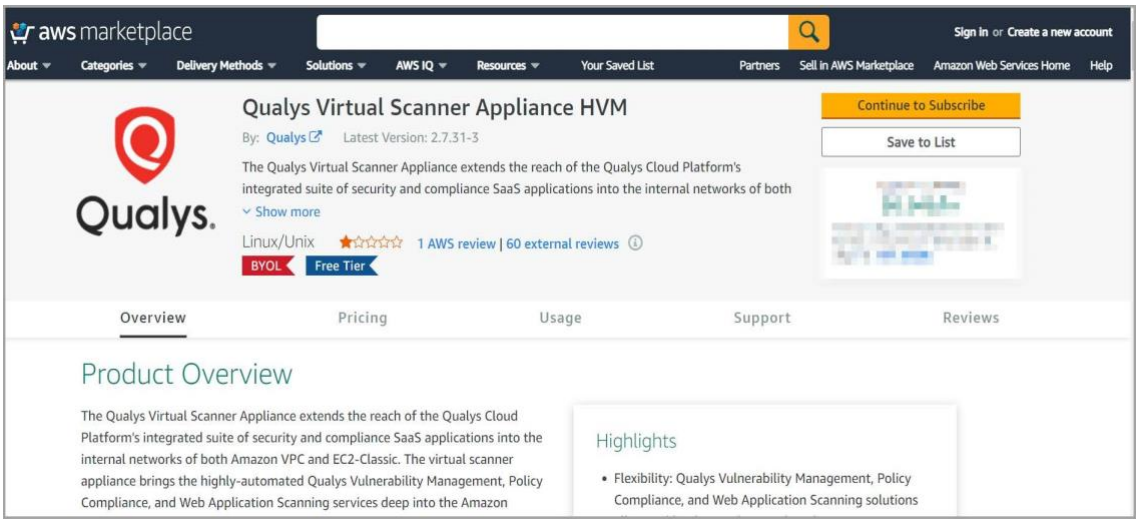
Qualys 仮想スキャナは、AWS マーケットプレイスから、または AWS アカウントと共有されているカスタム AMI から起動できます。AWS Management Console を使用して AMI インスタンスを起動することもできます (つまり、コンソールにサインインし、[サービス] > EC2 に移動して、以下の AMI 設定を入力します)。

1) Qualys Virtual Scanner Appliance を展開します。

AWS Marketplace から起動するには

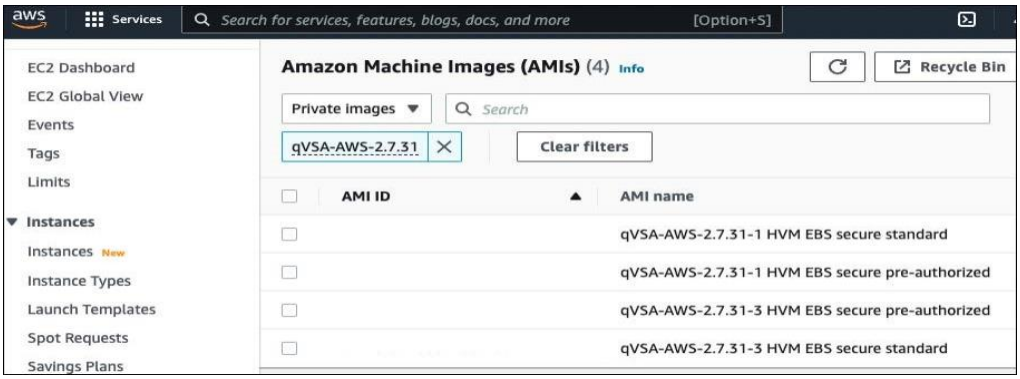
AWS Marketplace の Qualys Virtual Scanner Appliance ページに移動し、AWS アカウントにログインします。

AWS Marketplace の Qualys Virtual Scanner Appliance HVM



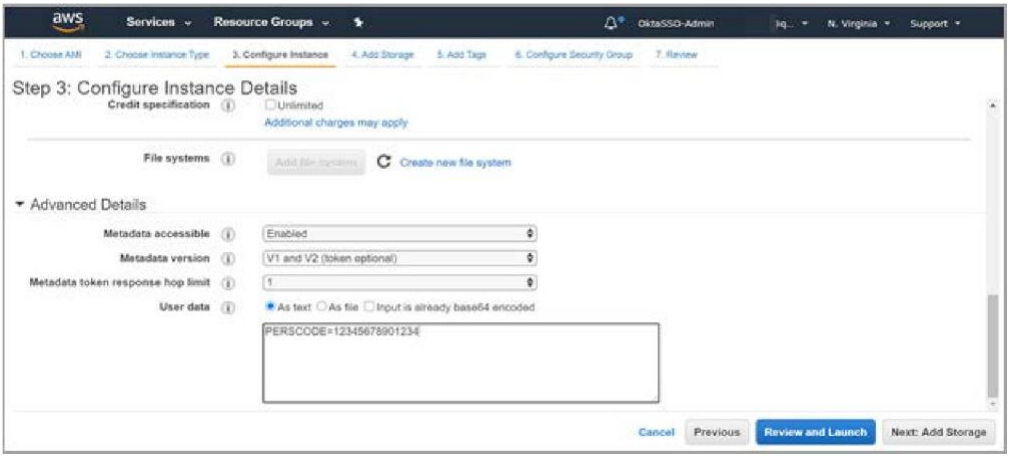
カスタム AMI を AWS コンソールから起動するには

AWS アカウントと共有されているカスタム AMI から起動するには、AWS コンソールにログインし、[Images] - [AMI] – [Private Images] に移動し、検索ボックスに「qVSA」と入力すると、アカウントで共有されているすべての Qualys 仮想スキャナイメージが表示されます。



2) リージョンで仮想スキャナ AMI を起動します。

3)ウィザードを使用して AMI 設定を入力します。Qualys は V2 (トークンが必要) バージョンもサポートするようになりました。[詳細] セクションで、それに応じて [メタデータ バージョン] を選択します。そのため、[ユーザー データ] フィールドに、Qualys ユーザー インターフェイスから取得したパーソナライゼーション コードと、必要に応じてプロキシ サーバー(使用する場合)を入力する必要があります。



パーソナライゼーションコード - Qualys から取得したパーソナライゼーションコードに、PERSCODE=を前に付けて入力します。

プロキシサーバー(オプション) - パーソナライゼーションコードとは別の行に、PROXY_URL を前に付けてプロキシサーバー情報を入力します。プロキシ サーバは、スキャナが Qualys Cloud Platform に直接接続できない場合に使用されます。

username:password@proxyhost:port の形式でプロキシ情報を入力します。
ドメイン ユーザーの場合、形式は domain\username:password@proxyhost:port です。
認証を使用しない場合、形式は proxyhost:port です

ここで、proxyhost はプロキシ サーバーの IPv4 アドレスまたは FQDN、port はプロキシ サーバーが実行されているポートです。

例：

```
PERSCODE=12345678901234
PROXY_URL=jdoe:abc12345@10.40.1.123:3128
```

プロキシサーバーを使用する場合は、Qualys UI で Amazon EC2 API プロキシサーバー設定を構成してください。詳細については、「Qualys UI での Amazon EC2 API プロキシ設定の定義」を参照してください。

クラウドシェルを使用して AWS クラウドに Qualys Virtual Scanner Appliance をデプロイする

次の AWS CLI コマンドは、AWS クラウドインフラストラクチャにインスタンスを作成します。「user-data」オプションでは、PERSCODE とプロキシサーバーの構成(存在する場合)を base64 でエンコードされた形式で指定する必要があることに注意してください。

次のコマンドを使用します。

aws ec2 run-instances [オプション] 必須パラメータ:

--image-id (文字列)

AMI の ID。インスタンスを起動するには AMI ID が必要であり、ここで指定するか、起動テンプレートで指定する必要があります。

--instance-type (文字列)

インスタンスタイプ。詳細については、「 Amazon EC2 ユーザーガイドのインスタンスタイプ」を参照してください。

- キー名 (文字列)

キーペアの名前。キーペアは、 CreateKeyPair または ImportKeyPair を使用して作成できます。

注:- キーペアを指定しない場合は、ユーザーが別の方法でログインできるように設定された AMI を選択しない限り、インスタンスに接続できません。

--security-group-ids (リスト)

セキュリティ グループの ID。CreateSecurityGroup を使用してセキュリティ グループを作成できます。

--subnet-id (文字列)

[EC2-VPC]インスタンスを起動するサブネットの ID。

ネットワーク・インターフェースを指定する場合は、ネットワーク・インターフェースの一部としてサブネットを指定する必要があります。

--user-data (文字列)

インスタンスで使用できるようにするユーザーデータスクリプト。詳細については、「起動時に Linux インスタンスでコマンドを実行する」および「起動時に Windows インスタンスでコマンドを実行する」を参照してください。コマンドラインツールを使用し

ている場合は、base64 エンコーディングが実行され、ファイルからテキストを読み込むことができます。それ以外の場合は、base64 でエンコードされたテキストを指定する必要があります。ユーザー データは 16 KB に制限されています。

AWS CLI を使用して Qualys スキャナを起動する例:

aws ec2 run-instances --image-id ami-07581f2a1fbf34f4f --count 1 --instance-type t1.micro --key-name vScanner --subnet-id subnet-81e1e5da --security-group-ids sg-0e6a6c4c16488fd6f –user-data UEVSU0NPREU9MTIzNDU2Nzg5MDEyMzQKUFJPWFlfVVJMPWFiYzp4eWRAMS4xLjEuMTo4MDgw

AWSクラウドインフラストラクチャでのインスタンスの起動の詳細については、https://awscli.amazonaws.com/v2/documentation/api/latest/reference/ec2/runinstances.html を参照してください。

起動すると、仮想アプライアンスは Qualys Cloud Platform に接続します

この手順では、Virtual Scanner Appliance を Qualys アカウントに登録します。また、アプライアンスは最新のソフトウェアアップデートをすべてすぐにダウンロードするため、スキャンの準備が整います。

Virtual Scanner Appliance のセキュリティグループの設定

Scanner Appliance に割り当てられたセキュリティグループでのアウトバウンドルールに従ったセットアップ。

13) Qualys Cloud Platform への接続

Scanner Appliance は Qualys Cloud Platform に接続できる必要があります。Scanner Appliance がインターネットに直接接続されている場合は、アウトバウンドルールでポート 443 から Qualys Security Operations Center(SOC)の IP アドレスへのアクセスが許可されていることを確認します。SOC の IP アドレス範囲を取得するには、Qualys ポータルにログインし、[ヘルプ] > [バージョン情報] オプションに移動します。プロキシ サーバを使用している場合は、プロキシ サーバへの通信を許可するアウトバウンド ルールがあり、プロキシ サーバが Qualys Cloud Platform に到達できることを確認します。

14) Amazon EC2 API エンドポイントへの接続

Scanner Appliance は、Amazon EC2 および STS API エンドポイントに接続できる必要があります。承認のためには、スキャナーは STS エンドポイントに到達してロールを引き受け、EC2 API 呼び出しを行うためのトークンを取得する必要があります。EC2 および STS API への通信は、アプライアンス管理用に構成したプロキシ サーバーを経由しません。

Qualys Cloud Platform との通信(上記参照)。Scanner Appliance は、EC2 および STS API と直接通信するか、完全に透過的なプロキシまたはフィルタリングテクノロジーを介して通信する必要があります。

Scanner Appliance がインターネットに直接接続されている場合は、アウトバウンドルールでポート 443 から Amazon EC2 および STS API エンドポイントへのアクセスが許可されていることを確認します。Qualys UI で Amazon EC2 API プロキシ サーバを設定した場合は、プロキシ サーバへの通信を許可するアウトバウンド ルールがあり、プロキシ サーバが Amazon EC2 API エンドポイントに到達できることを確認します。

Scanner Appliance は、Amazon EC2 API エンドポイントに接続できる必要があります。アプライアンスが Amazon EC2 API エンドポイントに到達できない場合、開始した EC2 スキャンジョブは成功しません。アプライアンスはターゲットインスタンス ID のリストを IP アドレスに解決できず、「No Hosts alive」というエラーが表示される可能性があるため、EC2 インスタンスターゲットをスキャンせずにスキャンが終了します。

リージョンとエンドポイントについては、こちらをご覧ください。
http://docs.aws.amazon.com/general/latest/gr/rande.html#ec2_region

- ターゲットインスタンスへの接続

スキャナーは、スキャンを実行するためにすべてのターゲット
インスタンスに到達できる必要があります。スキャナーがスキャンする EC2
インスタンスのすべてのポートとサブネットへのアクセスを許可するアウトバウンドルールを設定することをお勧めします。

Qualys プライベートクラウドプラットフォームのサポート

Qualys Private Cloud Platform(PCP)を使用して EC2 インスタンスをスキャンする場合は、Qualys 営業担当者(TAM)またはサポートに連絡して、AWS の仮想 Scanner Appliance AMI を生成してください。次の情報を入力します。

15) Scanner Appliance を導入する AWS リージョン

16) スキャナーのデプロイに使用する AWS アカウント

セキュリティグループが、ポート 443 で Scanner Appliance から Qualys PCP への通信を許可していることを確認します。Qualys PCP の IP アドレスをサポートに提供する必要がある場合があります。

Qualys Cloud Agent の展開

革新的な Qualys Cloud Agent プラットフォームを使用すると、軽量のクラウドエージェントを導入して、AWS インフラストラクチャのセキュリティとコンプライアンスを継続的に評価できます。

Cloud Agent の機能

17) ポート 443 経由で Qualys Cloud Platform と通信し、プロキシ設定をサポートします。

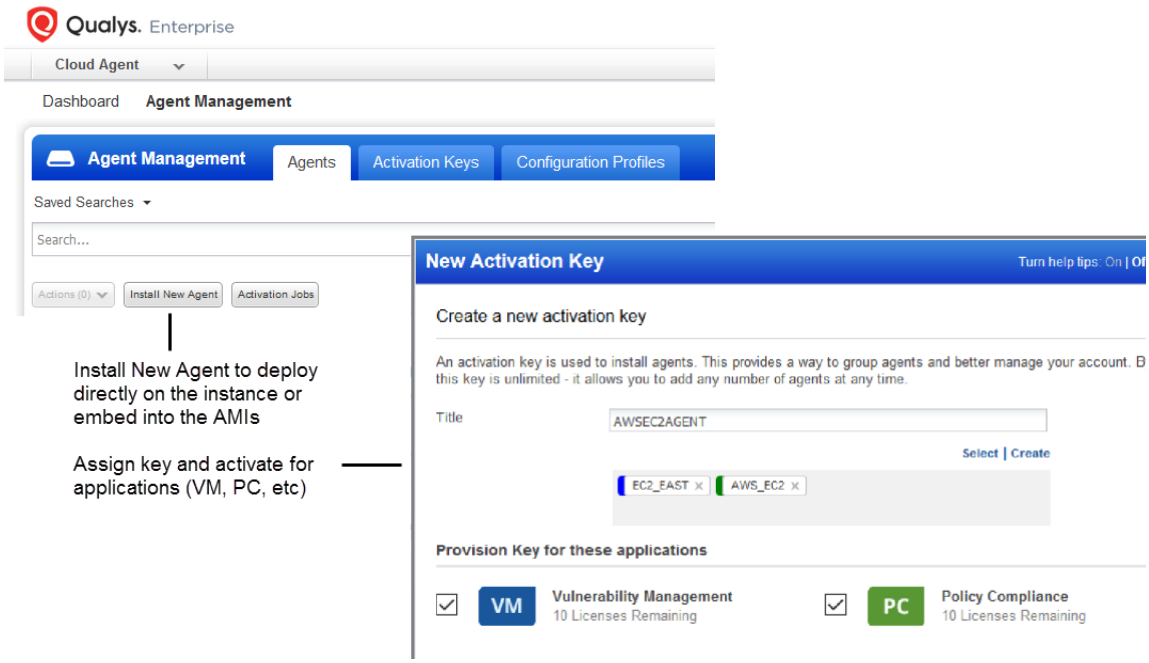
18) EC2 インスタンスに直接デプロイすることも、AMI に埋め込むこともできます。クラウドバーストとエフェメラルインスタンスに適しています

19) さまざまな Linux および Windows OS バージョンのスキャンをサポート

20) EC2 インスタンス OS の脆弱性のスキャンをサポート

どのような手順ですか?

Cloud Agent(CA)アプリに移動し、数分でCloud Agentをインストールします。



次のリソースをお勧めします

Qualys Cloud Platform

Qualys Cloud Agent Getting Started Guide

アセットのスキャン

ネットワークをスキャンする手順が表示されます。スキャンを開始する前に、いくつかのチェックポイント/事前設定を確認する必要があります。

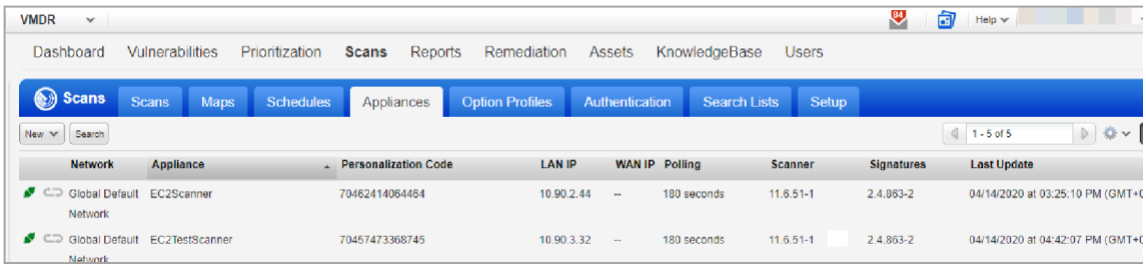
EC2 スキャンチェックリスト

[Qualys VM/VMDR] または [Qualys PC] に移動します - スキャンする前に、次の手順をお勧めします。

- Check Appliance Status
- Define Amazon EC2 API Proxy settings in Qualys UI (プロキシサーバーを定義した場合のみ)
- Check EC2 Assets are activated
- Configure security groups for the EC2 instances to be scanned
- Configure OS Authentication

アプライアンスのステータスの確認

[Scans > Appliances (アプライアンスのスキャン)] に移動します - 新しい Scanner Appliance が Qualys Cloud Platform に接続されていることを確認します。



の意味は、アプライアンスが接続され、スキャンの準備が整っていることを意味します。

Qualys UI での Amazon EC2 API プロキシ設定の定義

このステップは、仮想スキャナーのデプロイメント中に「ユーザー・データ」フィールドにプロキシー・サーバーを定義した場合に必要です。このステップを実行しないと、EC2 スキャンは機能しません。

[Scans > Appliances - Edit your EC2 Virtual Scanner Appliance (アプライアンスのスキャン - EC2 仮想スキャナアプライアンスの編集)] に移動します。[プロキシ設定] タブに移動し、[Amazon EC2 API プロキシ] チェックボックスをオンにして、プロキシサーバーにつ

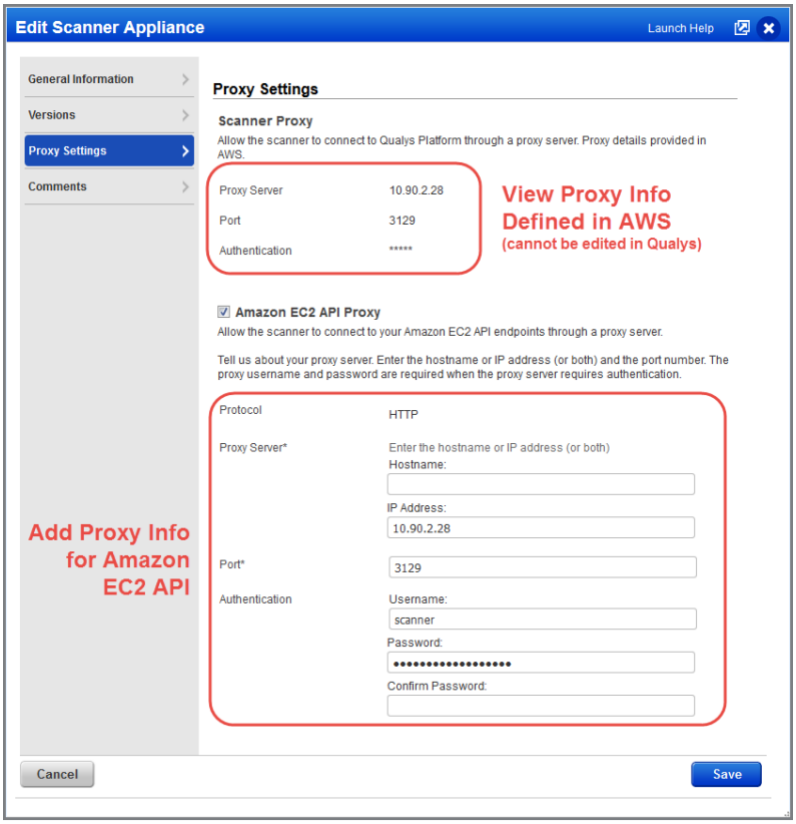
いて (ホスト名や IP アドレス、ポート、プロキシ認証情報 (プロキシサーバーで必要な場合) など) をお知らせください。

知っておきたいこと - ここで入力する設定により、仮想アプライアンスは Amazon EC2 API エンドポイントに接続できます。仮想アプライアンスは、指定したプロキシサーバーを介して AWS Gateway への API 呼び出しを行います。たとえば、DescribeInstance API を呼び出して、スキャンする各 EC2 インスタンスの現在の IP アドレスを取得します。

Scanner Appliance のプロキシ設定の例

すべてのプロキシ設定は、Scanner Appliance の情報ページで確認できます。[Scans > Appliances]に移動し、アプライアンスにカーソルを合わせて、[クイックアクション]メニューから[情報]を選択します。[編集] をクリックして、Amazon EC2 API プロキシの設定を変更します。

[Scanner Proxy] セクションには、デプロイ中に AWS AMI 設定で現在定義されているプロキシサーバー情報が表示されます (認証情報は *** でマスクされます)。

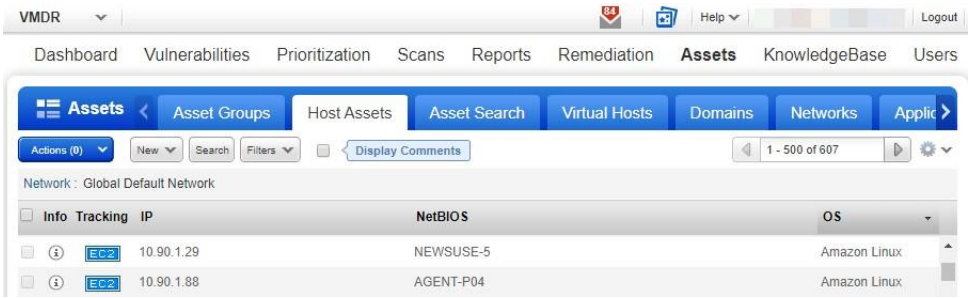


EC2 リージョンエンドポイントにプロキシ経由でアクセスできるようにする必要があります。

ここからエンドポイントへの URL を特定します。
http://docs.aws.amazon.com/general/latest/gr/rande.html#ec2_region

EC2 アセットがアクティブ化されていることを確認する

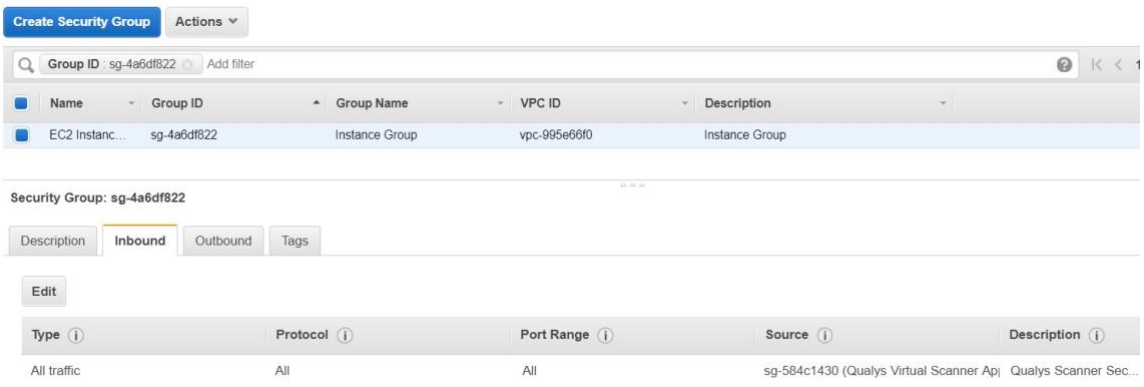
[Assets] > [Host Assets] または [Qualys AssetView (AV)] に移動します。 - EC2 ホストがアクティブ化されていることを確認します。アクティブ化されたアセットには、EC2 追跡方法が割り当てられます。



スキャンする EC2 インスタンスのセキュリティグループを設定する

AWS では、Scanner Appliance の IP アドレスまたは Scanner Appliance のセキュリティグループのすべてのポートでインバウンドアクセスを許可するセキュリティグループを関連付ける必要があります。

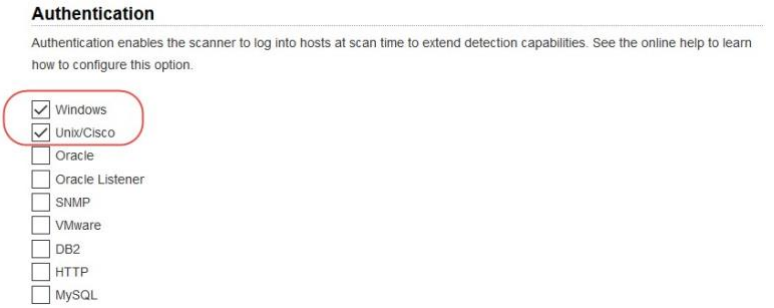
以下は、Qualys Virtual Scanner Appliance のセキュリティグループのすべてのポートでインバウンドアクセスを許可する EC2 インスタンスに割り当てられたセキュリティグループの例です。



OS 認証の構成

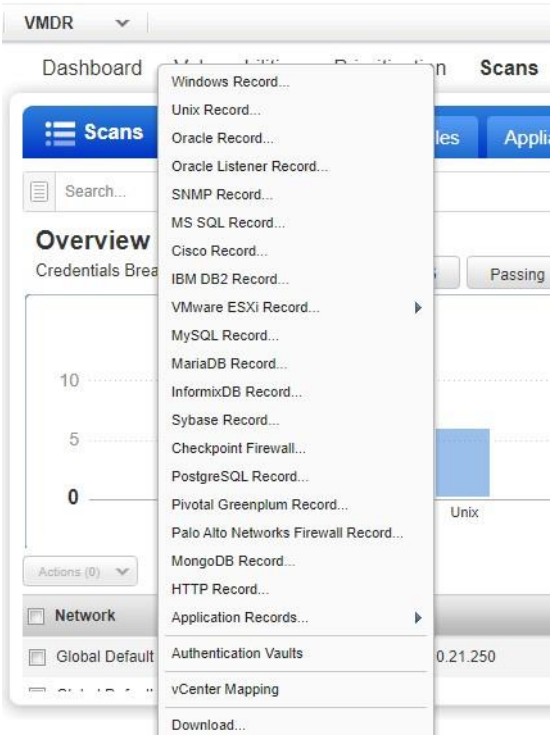
ホスト OS 認証(トラステッドスキャン)を利用することで、スキャン中に各ターゲットシステムにログインすることができます。認証済みスキャンを実行すると、誤検知が少なく、最も正確な結果が得られます。

「スキャン」>「オプション・プロファイル」に移動します。プロファイルの初期オプションを編集し、[名前を付けて保存]を使用してコピーを別の名前で保存します。新しいプロファイルで、必要な認証の種類を有効にします。



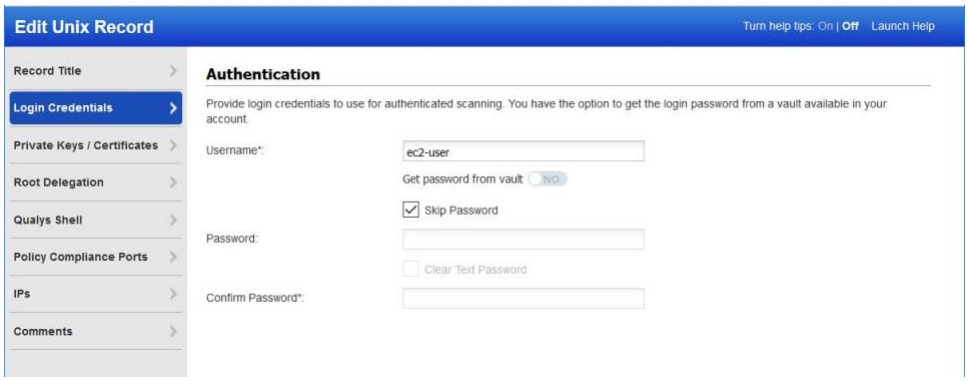
「スキャン>認証」に移動します。スキャンする EC2 インスタンス (Unix や Windows) の認証レコードを追加します。レコードには、認証に使用するアカウントの資格情報を追加する必要があります - これは OS ユーザー (AIM ユーザーではない) のアカウントです。

ターゲット システムでの認証専用のアカウントを作成することをお勧めします。



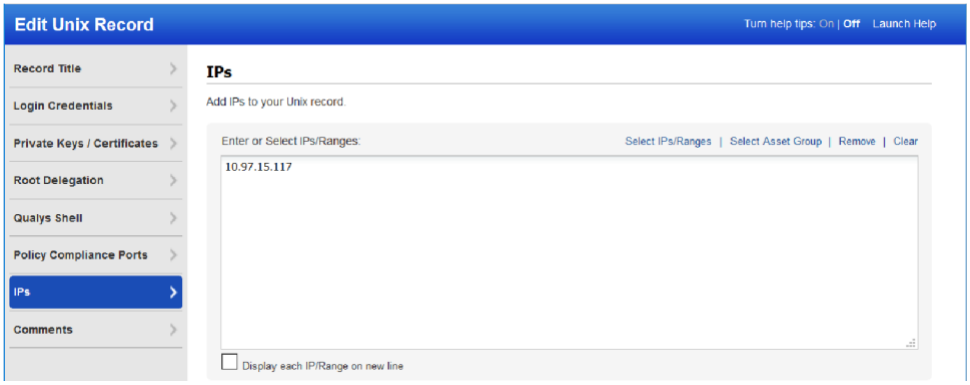
サンプル Unix レコード

1) ログイン資格情報 - OS ユーザー名を入力し、[パスワードをスキップ]を選択します。



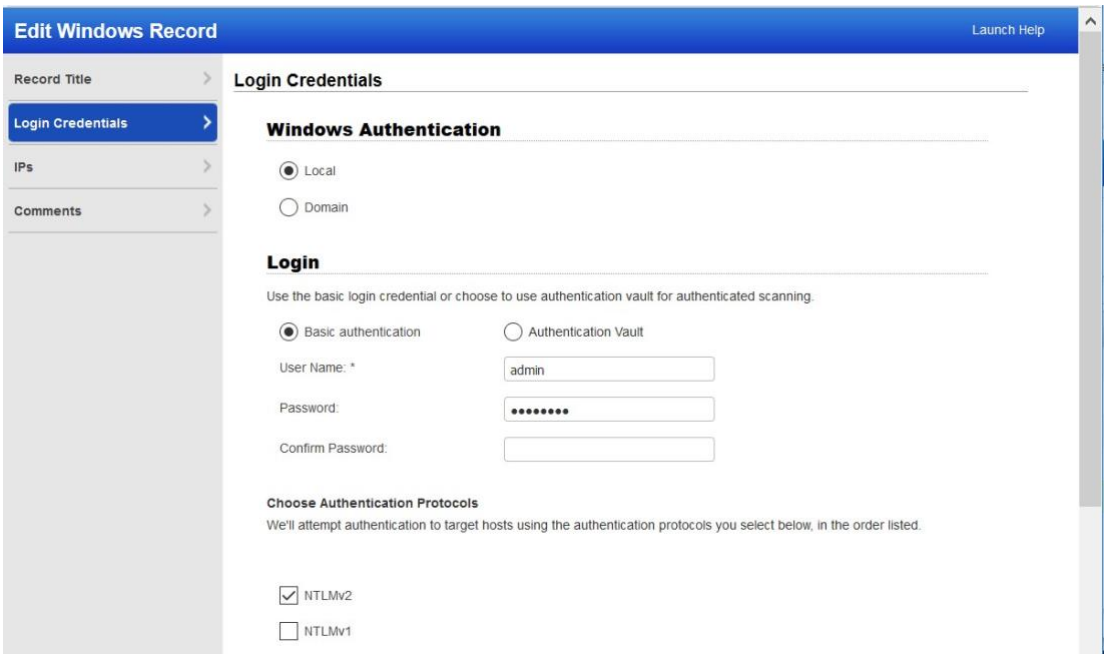
2) 秘密キー - キー認証をお勧めします。キーの種類 (RSA、DSA、ECDSA、ED25519) を選択し、秘密キーの内容を入力します。

3) IP - このレコードの EC2 インスタンスの Unix IP アドレス/範囲を選択します。このレコードの資格情報は、これらのアセットのスキャンに使用されます。

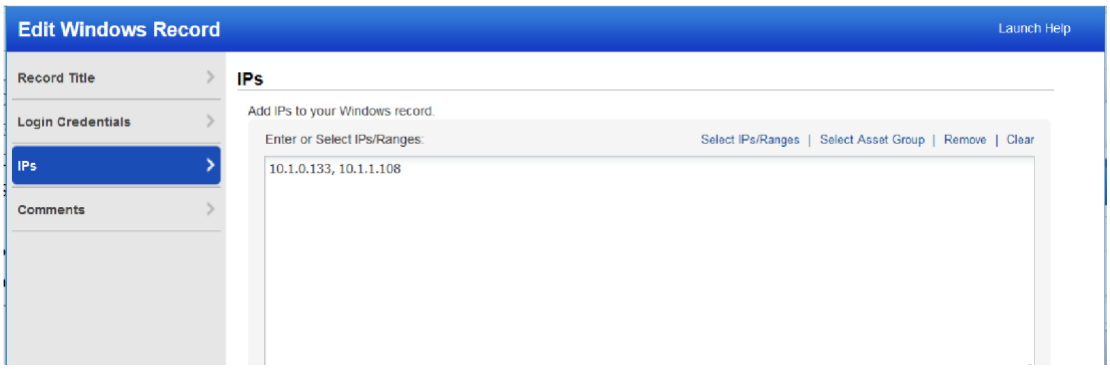


サンプル Windows レコード

1) ログイン資格情報 - OS ユーザー名を入力し、[パスワードをスキップ]を選択します。



2) IP - このレコードの EC2 インスタンスの Windows IP アドレス/範囲を選択します。このレコードの資格情報は、これらのアセットのスキャンに使用されます。



OS 認証の詳細

認証レコードのワークフロー内のオンラインヘルプには、使用可能なすべてのオプションに関する詳細な手順とガイダンスが表示されます。これらのドキュメントは優れたリソースです。

Qualys Windows 認証ガイド (pdf)

Qualys Unix 認証ガイド (pdf)

Qualys はネットワークを定義していますか？ 仮想アプライアンスの移動

この手順は、Qualys アカウントでカスタム ネットワークを定義している場合に推奨されます。

デフォルトでは、新しい仮想 Scanner Appliance は [グローバルデフォルト(Global Default)] に配置されます。

ネットワークとスキャンが実行されると、ホストのスキャンデータがそのネットワークに追加されます。スキャンする前に、この仮想アプライアンスを目的のネットワーク(グローバル EC2 ネットワークまたはカスタムネットワーク)に移動することをお勧めします。

[アセット] > [ネットワーク] に移動し、仮想アプライアンスの移動先のネットワークを編集して、アプライアンスをそのネットワークに追加します。

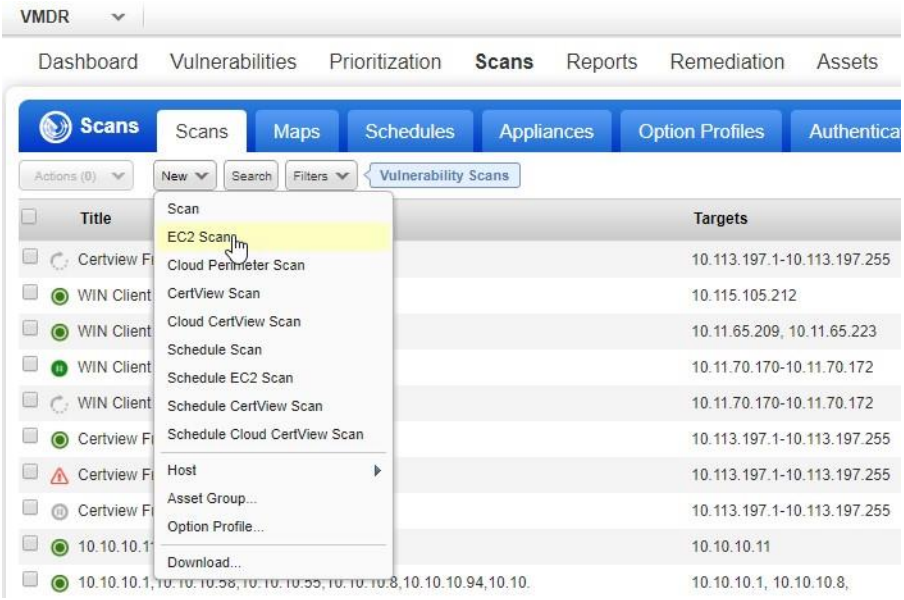
Virtual Scanner Appliance を使用したスキャン

Virtual Scanner Appliance を使用したスキャンには、次の一連の手順が含まれます。

EC2 スキャンワークフロー

Qualys は、スキャン仮想アプライアンス AMI のインスタンスと連携する場合にのみ機能する特別な EC2 スキャン (および EC2 スキャンのスケジュール) ワークフローを提供します。このソリューションでは、Amazon EC2-Classic および EC2-VPC でオンデマンドおよびスケジュールされたスキャンが可能になり、お客様が AWS にスキャン許可を手動でリクエストする必要はありません。

Qualys コミュニティ: AWS Acceptable Use Guidance For Scanning (スキャンに関する AWS 利用規定のガイダンス)



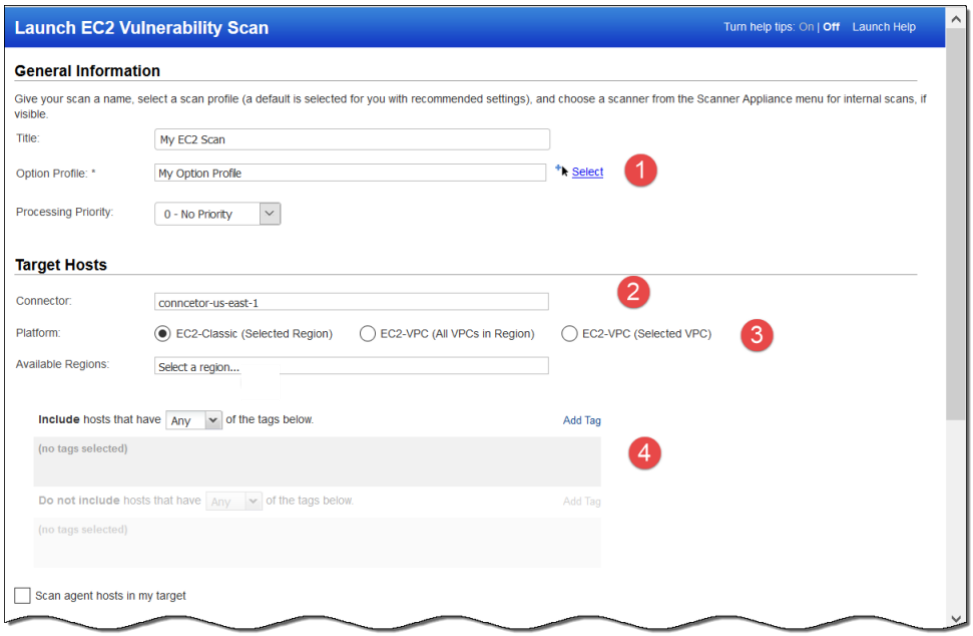
スキャン設定を指定します。

1) スキャンにタイトルを付け、認証で構成したオプションプロファイルを選択します (脆弱性スキャンに必要)。

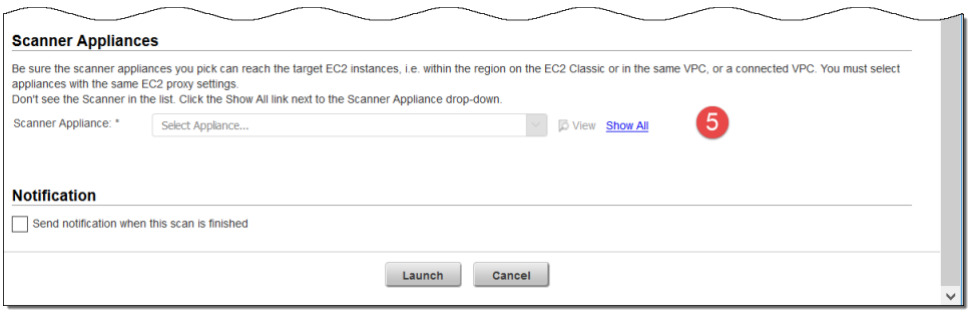
2) 構成した EC2 コネクタ名を選択します。

3) [プラットフォーム] で、[EC2 Classic]、[EC2 VPC] (リージョン内のすべての VPC)、または [EC2 VPC] (選択した VPC) のいずれかを選択します。選択内容に基づいて、地域を選択します。

4) アセットタグの選択 - これらは、コネクタに対してアクティブ化されたアセットです。

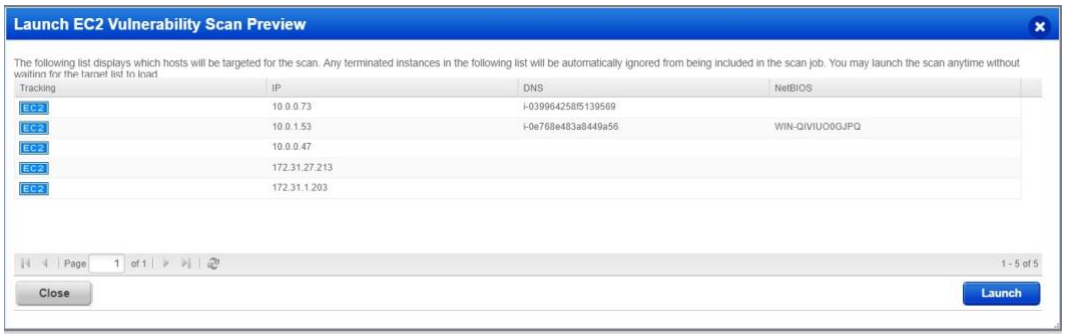


5) Amazon EC2 で起動した Virtual Scanner Appliance AMI を選択します。



6) [起動] をクリックして、Amazon EC2 インフラストラクチャのスキャンと保護を開始します。

スキャンを開始する前に、EC2 脆弱性スキャンプレビューにはすべてのインスタンス (終了したインスタンスを含む) が一覧表示されます。ただし、スキャン中は、このような終了したインスタンスはすべてスキャンから無視されます。

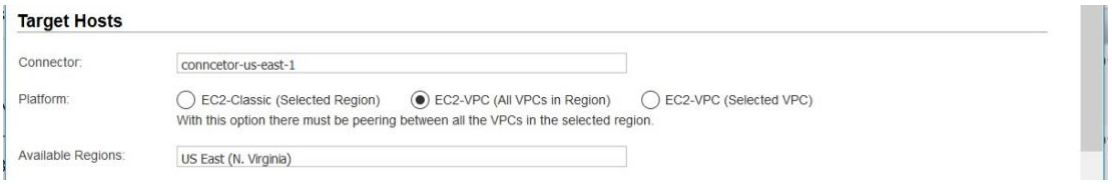


EC2 Classic インスタンスのスキャン

リージョン内の EC2 クラシックホストをスキャンするには、**[EC2 Classic (Selected Region)]** を選択します。選択すると、リージョン内の EC2 Classic インスタンスのみがスキャンされます。

VPC インスタンスのスキャン

選択した **VPC のみをスキャンするには、[**EC2-VPC (Selected VPC)] を選択します。



VPC ピアリングを使用したインスタンスのスキャン

リージョン内のすべての VPC をスキャンするには、**[EC2-VPC (All VPCs in Region)]** を選択します。このオプションは、リージョン内のすべての VPC 間にピアリングがある場合のみ選択してください。そうしないと、Virtual Scanner Appliance が到達できないインスタンスで「ホストが見つかりません」というエラーが発生する可能性があります。

GovCloud での EC2 インスタンスのスキャン

Qualys Virtual Scanner Appliance(qVSA)を使用して AWS GovCloud の保護を開始するには、以下の手順に従ってください。

1) Qualys TAM または Qualys サポートに連絡して、a) GovCloud 機能および b) Qualys 仮想スキャナアプライアンス AMI へのアクセスをリクエストしてください。

2) スキャナーを実行する AWS アカウント ID を含めると、AMI へのアクセスは、特定のアカウント ID に対する Qualys サポートによって有効になります。

3) Qualys サポートから、承認とアクセス情報が記載されたメールが送信されます。

4) 「qVSA」AMI を使用して Qualys 仮想スキャナ インスタンスを作成すると、インスタンスの作成ウィザードの [MyImages] セクションで使用できるようになります。(検索する必要がある場合は、キーワード「qVSA」を使用して Qualys スキャナーを見つけます)。

5) 「スキャナの展開」の説明に従って仮想スキャナインスタンスを設定します

6) スキャンを開始する準備が整いました。「Virtual Scanner Appliance を使用したスキャン」の手順に従ってください。

Qualys Cloud Agent を使用した内部ネットワークスキャン

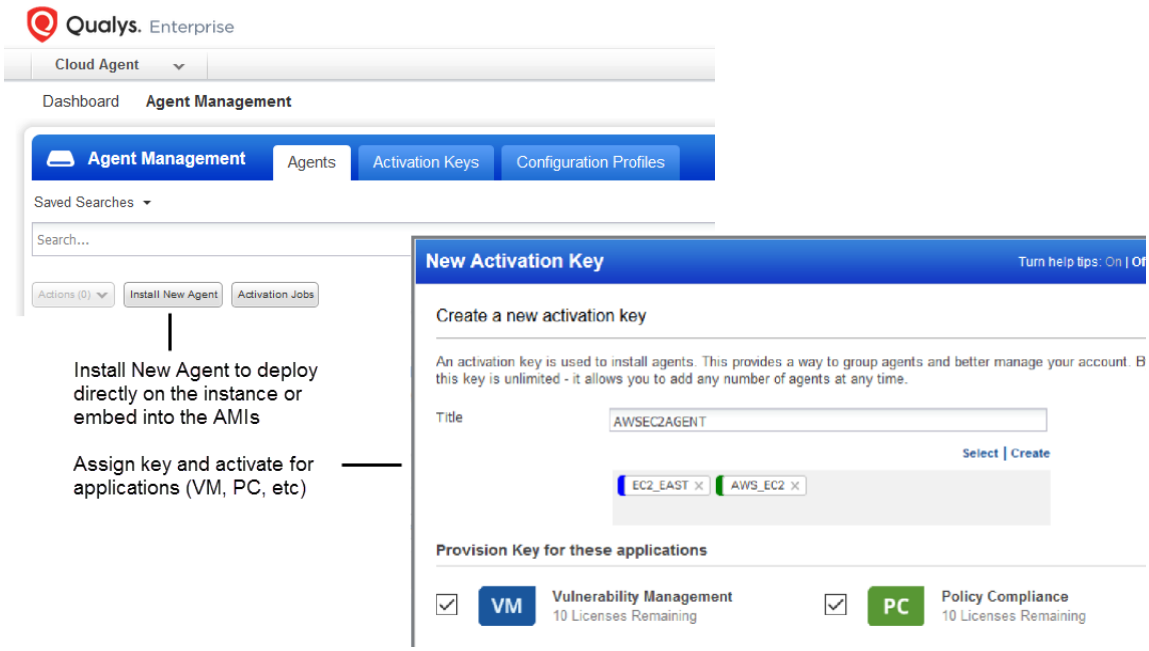
革新的な Qualys Cloud Agent プラットフォームを使用すると、軽量のクラウドエージェントを導入して、AWS インフラストラクチャのセキュリティとコンプライアンスを継続的に評価できます。

Cloud Agent の機能

- ポート 443 経由で Qualys Cloud Platform と通信し、プロキシ設定をサポートします。
- EC2 インスタンスに直接デプロイすることも、AMI に埋め込むこともできます。クラウドバーストとエフェメラルインスタンスに適しています
- さまざまな Linux および Windows OS バージョンのスキャンをサポート
- EC2 インスタンス OS の脆弱性のスキャンをサポート

はじめに

Cloud Agent(CA)アプリに移動し、数分で Cloud Agent をインストールします。



次のリソースをお勧めします。

Qulays Cloud Platform

Qualys Cloud Agent Getting Started Guide

Qualys スキャナーを使用したペリメータスキャン

Qualys Cloud Platform にある Qualys スキャナ(インターネット リモート スキャナ)は、EC2 インスタンスのペリメータスキャンに使用できます。

プライベート クラウド プラットフォームのサブスクリプションの場合、内部スキャナーの使用を許可するようにアカウントが構成されている場合があります。

これらは、ターゲット EC2 インスタンスのパブリック DNS またはパブリック IP を使用して開始された DNS または IP ベースのスキャンです。EC2 アセットにパブリック DNS とパブリック IP アドレスの両方が存在する場合は、パブリック DNS でスキャンが開始されます。

必要条件

Cloud Perimeter Scanning は、アカウントで次の機能が有効になっている場合に利用できます。

- EC2 スキャンと 2)ホスト名によるスキャン。
- アカウントには、次の権限が割り当てられたマネージャーまたはユニットマネージャーの役割が必要です。
- クラウドペリメータスキャンを有効にします (外部スキャナを使用してスキャンを開始します)。
- クラウドペリメータスキャンの内部スキャナを有効にします。(内部スキャナを使用してスキャンを開始する場合)

EC2 コネクタが必要です。スキャンに「コネクタのパブリックロードバランサーを含める」場合は、TotalCloud アカウントでこの同じ EC2 コネクタを構成します。コネクタを作成するには、アカウントに TotalCloud サブスクリプションがあり、プラットフォームにアクセスできる必要があります。

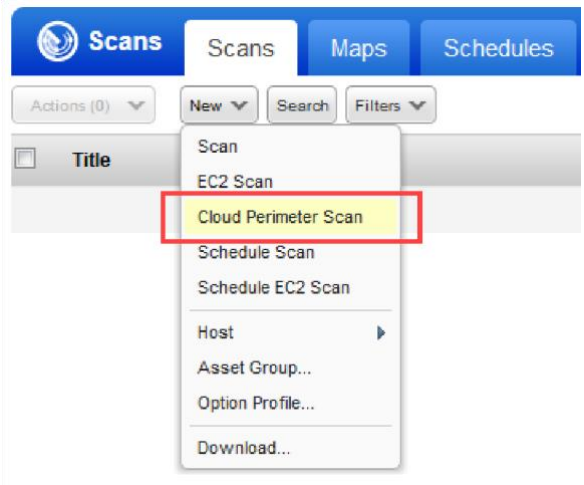
TotalCloud ベース URL「qweb_cloud_view_base_url」に。TotalCloud オンラインヘルプの「AWS コネクタの設定」を参照してください。

マイクロ、ナノ、スモールのインスタンスタイプをスキャンに含める場合は、これらのインスタンスタイプをアカウントでアクティブ化する必要があります。

はじめに

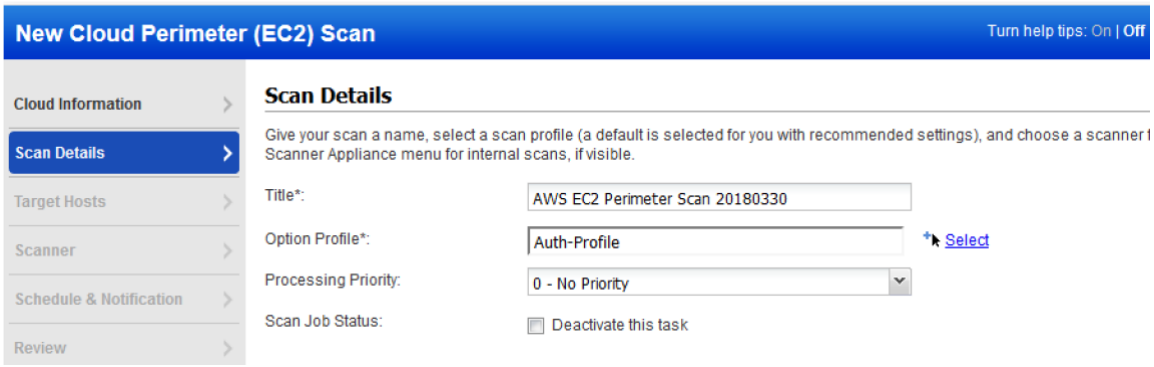
すべてのクラウドペリメータスキャンは、「今すぐ」(1 回限りのスキャンジョブ)または「繰り返し」のいずれかにスケジュールされます。保存すると、スキャン ジョブが [スケジュール] リストに表示されます。スキャン ジョブが開始されると、スキャン リストに表示されます。

脆弱性スキャンの場合は VM/VMDR (コンプライアンス スキャンの場合は PC) に移動し、[クラウドペリメータスキャン>新規作成] を選択します。このオプションは [スケジュール] タブにも表示されます。



最初に行うことは、構成した EC2 コネクタを選択することです。

スキャンにタイトルを付け、認証で構成したオプションプロファイルを選択します。認証されていないクラウド・ペリメータ・スキャンまたは認証されたクラウド・ペリメータ・スキャンのいずれかを起動できます。



次に、ターゲットホストを選択します。プラットフォーム、リージョン コード、VPC ID、アセット タグ、またはロード バランサーの DNS 名を指定しない場合は、コネクタから解決されたアセットのスキャンが開始されます。

(オプション)プラットフォームオプションとして、[EC2 Classic]、[EC2 VPC] (リージョン内のすべての VPC)、または [EC2 VPC] (選択した VPC) を選択します。選択内容に基づいて、地域を選択します。

また、インスタンスタイプが t2.nano、t3.nano、t1.micro、m1.small のアセットをスキャンに含めることもできます。このオプションを選択すると、これらのインスタンスタイプに対して認証やライトポートスキャンを実行しないことを推奨する警告メッセージが表示されます。マイクロ、ナノ、スモールのインスタンスタイプをスキャンに含めるには、これらのインスタンスタイプをアカウントでアクティブ化する必要があります。

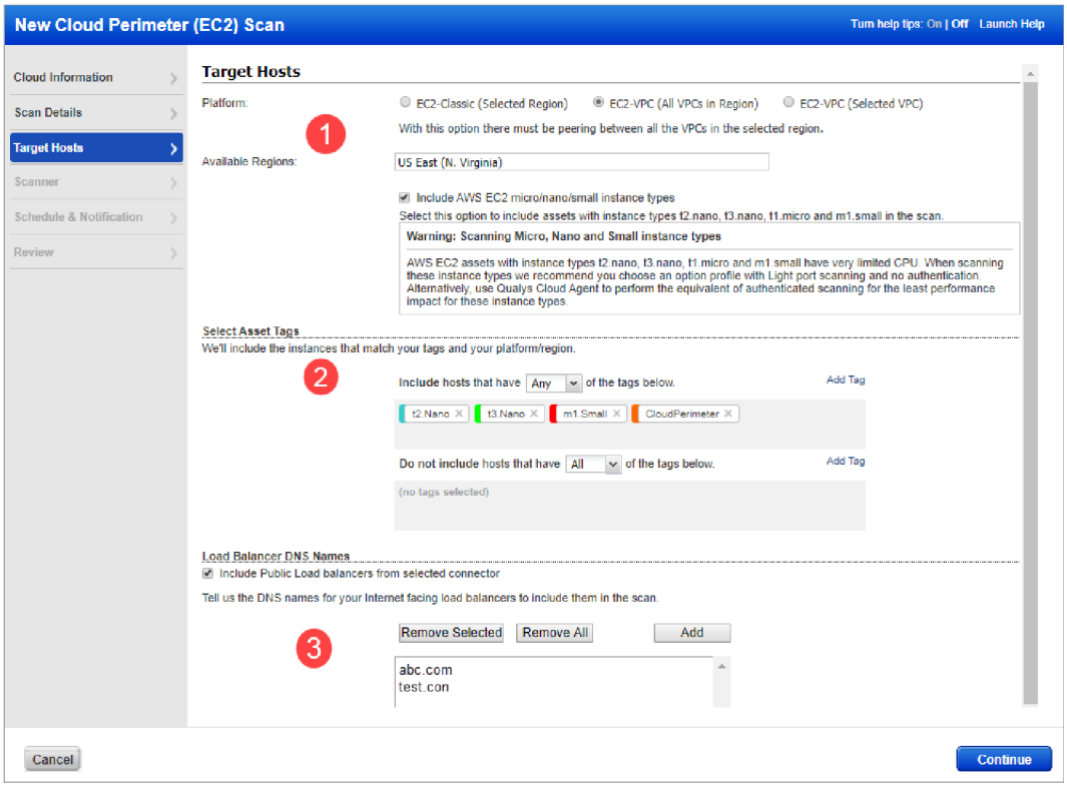
(オプション)アセットタグの選択 - これらは、コネクタに対してアクティブ化されたアセットです。

(オプション)「パブリック・ロード・バランサ」チェック・ボックスを選択して、選択したコネクタのパブリック・ロード・バランサを含めます。EC2 Classic プラットフォームは、パブリックロードバランサーをサポートしていません。

また、ロード・バランサの DNS 名を入力して、パブリック・ロード・バランサとともにスキャンに含めることもできます。[追加] をクリックして DNS 名を入力します。

[Include Public Load balancers from selected connector] チェックボックスをオンにすると、選択したコネクタと同じ構成の TotalCloud の AWS コネクタからパブリックロードバランサーが取得されます。このオプションを選択する場合は、選択したコネクタと同様の構成で TotalCloud アカウントにコネクタが作成されていることを確認してください。TotalCloud のコネクタが見つからない場合、このオプションを選択してもパブリックロードバランサーは取得されません。TotalCloud オンラインヘルプの「AWS コネクタの設定」を参照してください。

アセットとロードバランサーを解決するときに、アセットまたはパブリックロードバランサがコネクタから解決されず、オプションの「プラットフォーム」と「アセットタグ」を選択した場合は、ロードバランサーの DNS 名でスキャンが開始されます。ロードバランサーの DNS 名が指定されていない場合、スキャンは失敗し、終了します。

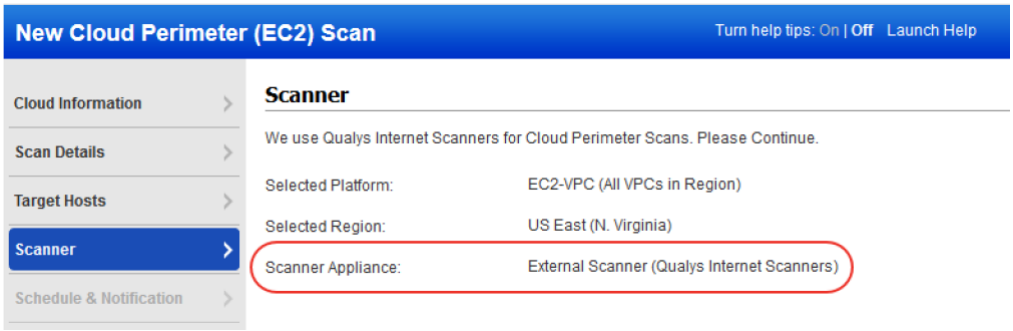


DNS ベースのスキャン

この機能は、サブスクリプションでオンにする必要があります。この機能を有効にする場合は、Qualys サポートにお問い合わせください。

DNS ベースのスキャンのしくみ: ユーザーは DNS で ELB などのスキャンを送信します。IP はリアルタイムで解決され、スキャンされます。

デフォルトでは、クラウドペリメータスキャンは Qualys 外部スキャナを使用します。

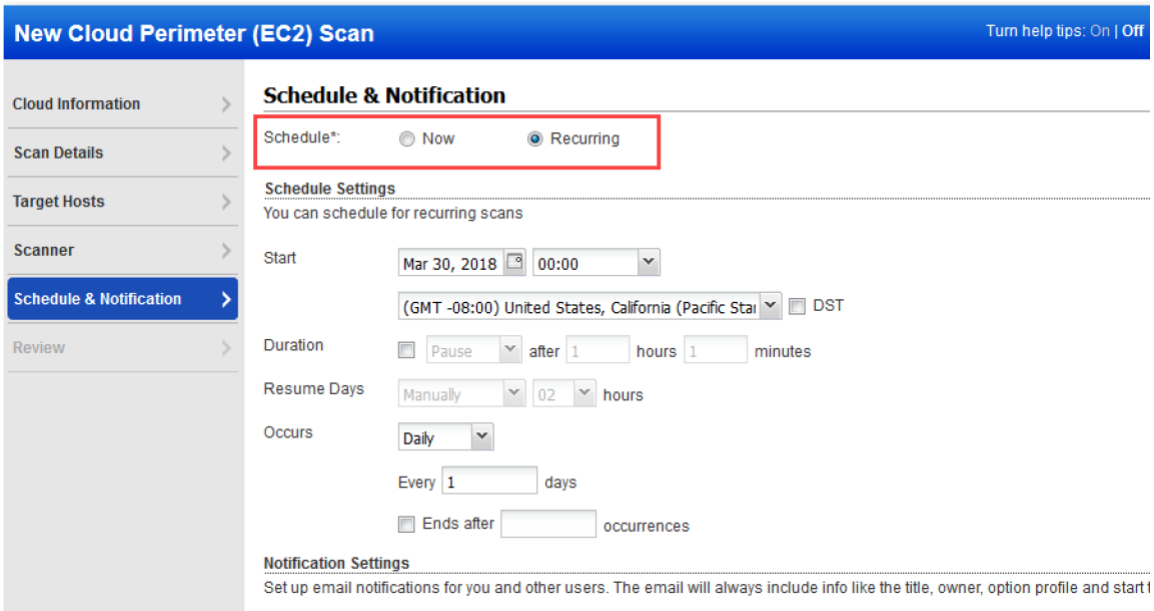


プライベート クラウド プラットフォームの場合 - サブスクリプションは、クラウドペリメータスキャン ジョブに Scanner Appliance を使用できるように設定できます。この場合、リストから 1 つ以上の Scanner Appliance を選択します([Build my list] オプションを使用します)。

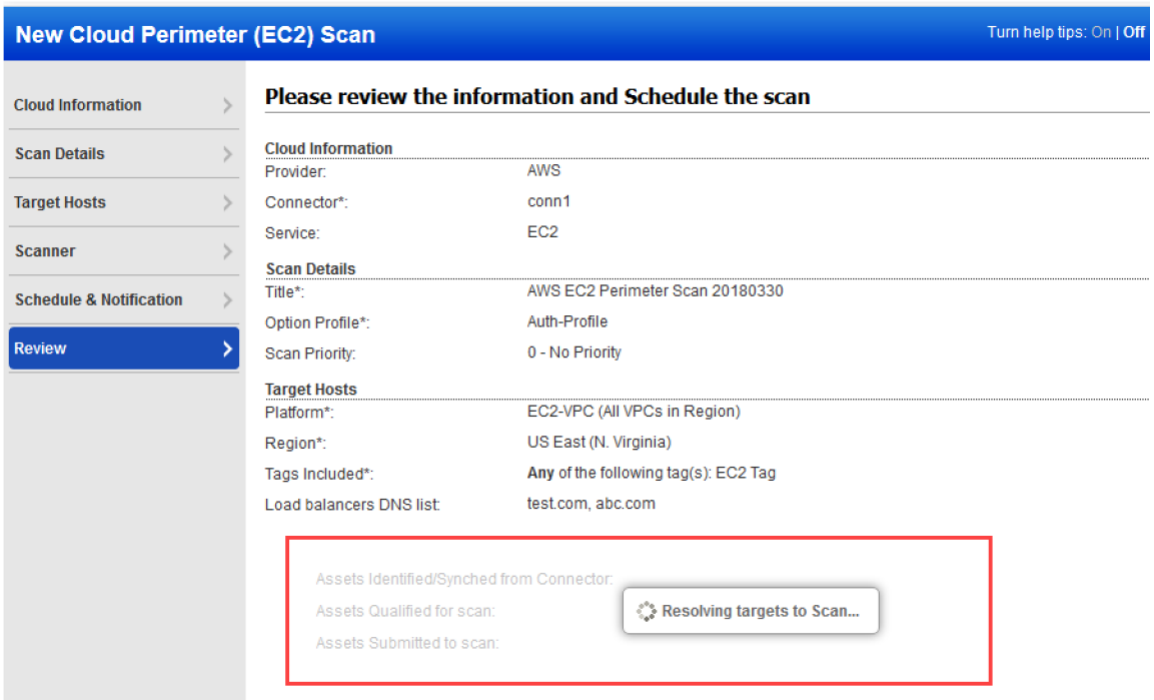
スキャンをいつ実行するか ([今すぐ] または [繰り返し]) を指定します。

[今すぐ] を選択すると、スキャンがすぐに開始されない場合があります。新しいスキャン要求は数分ごとにチェックされます。スキャナーが使用可能で、同時スキャンの制限に達していない場合は、スキャンが開始されます。スキャナーが使用できない場合、または制限に達した場合は、次の機会にスキャンが開始されます。

[定期的] を選択すると、スケジュール設定と通知オプションも設定されます。これらは他のスキャン スケジュールと同じ設定であるため、見覚えがあるはずです。



設定に基づいてスキャンするアセットが特定されます。



次のアセット数が表示されます。

識別/同期されたアセット - このスキャン ジョブ用に選択したコネクタによって検出されたアセットの数。

スキャンに適格なアセット - コネクタによって検出され、選択したプラットフォーム、リージョン、アセットタグにも一致するアセットの数。Terminated インスタンスを削除します。

スキャンに送信されたアセット - スキャン ジョブで送信されるアセットの数。認定されたアセット (以前の数) から開始し、VM に対してアクティブ化されていないアセット (脆弱性スキャンの場合) または PC に対してアクティブ化されていないアセット (コンプライアンス スキャンの場合) を除外します。

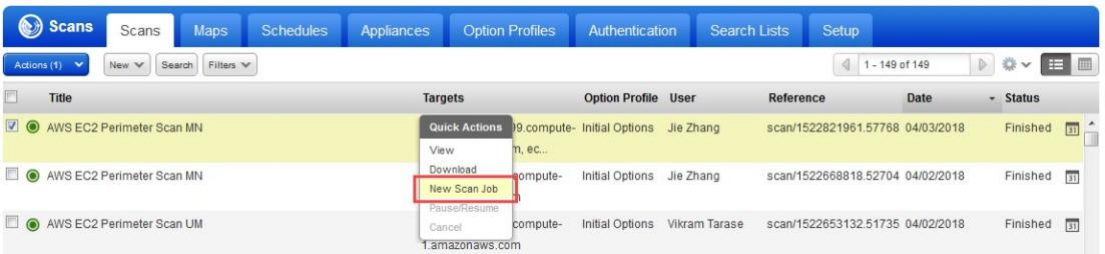
準備ができたら、「スキャン・ジョブの送信」をクリックします。

次に起こること

新しいスキャン ジョブが [スケジュール] リストに表示されます。

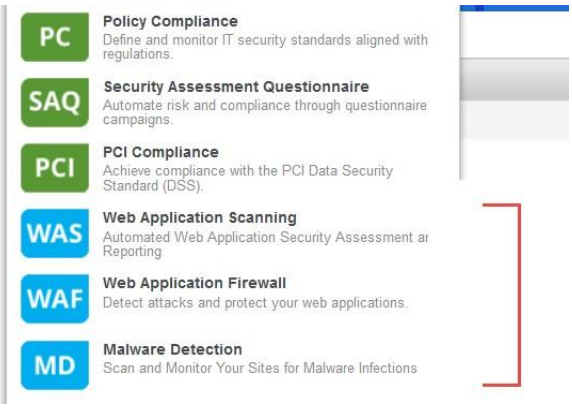
スキャンが開始されると、スキャンリストに表示されます。他のスキャンと同様に、スキャンのキャンセルや一時停止、スキャンの状態の表示、結果のダウンロードなどのアクションを実行できます。

スキャンをもう一度実行したいですか?[クイック アクション] メニューから [新しいスキャン ジョブ] を選択します。元のスキャン ジョブの特定のスキャン設定を保持し、スキャンを "今すぐ" 実行するようにスケジュールします。



Web アプリケーションのセキュリティ保護

Qualys を使用すると、アプリケーションスキャンおよびファイアウォールソリューションを使用してアプリケーションを保護できます。



Qualys WAS

Qualys Web Application Scanning(WAS)は、クロスサイトスクリプティング(XSS)や SQL インジェクションなどのアプリケーションや RESTAPI の脆弱性を特定するために、カスタム Web アプリケーションの自動クロールとテストを提供します。開始するには、Qualys Virtual Scanner Appliance をインストールします。これは、脆弱性とコンプライアンスチェックのスキャンに使用されるのと同じアプライアンスです。

どのように始めればよいですか?

7) 「スキャナーの展開」の手順に従います。

8) 次に、『Qualys Web Application Scanning Getting Started Guide』の手順を確認します。

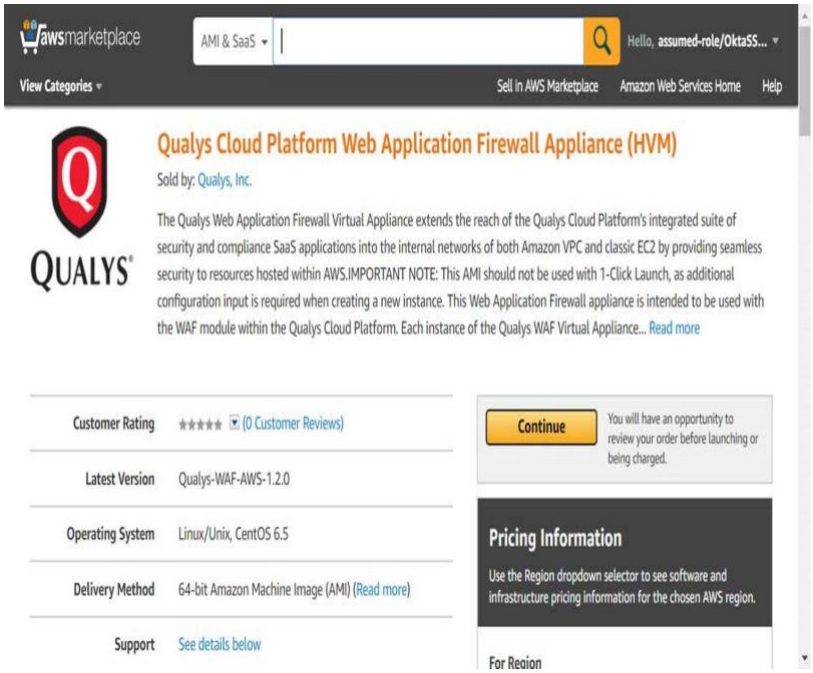
Qualys WAF

Qualys Web Application Firewall(WAF)を使用して、ファイアウォールルールとインスタント仮想パッチでアプリケーションを保護します。

どのように始めればよいですか?

- AWS Marketplace で入手可能な Web Application Firewall アプライアンスをインストールします。
- 次に、『Qualys Web Application Firewall Getting Started Guide』の手順を確認します。

AWS Marketplace の Qualys Cloud Platform Web Application Firewall Appliance (HVM)

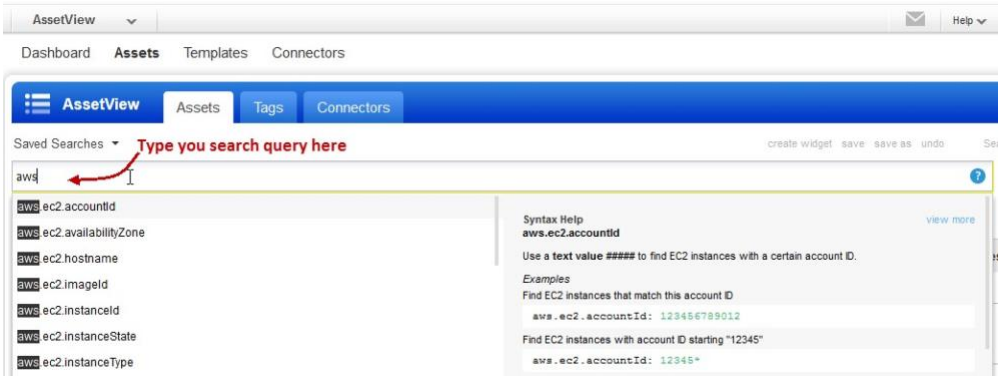


分析、レポート、修復

このセクションでは、アセットをクエリする方法、ウィジェットとダッシュボードを構築する方法、および脆弱性管理で AWS ホストに関するレポートを生成する方法について説明します。

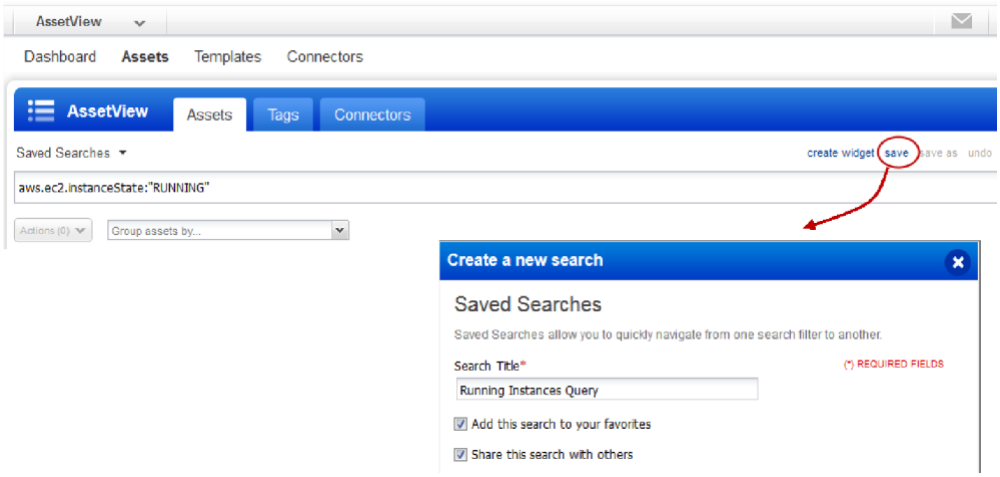
EC2 アセットをクエリする方法

当社の検索機能により、アセットに関するすべてのものを 1 か所ですばやく見つけることができます。AssetView アプリの Assets タブに移動します。「AWS」と入力すると、accountId、instanceType、hostname など、検索できるアセットプロパティが表示されます。興味のあるものを選択します。



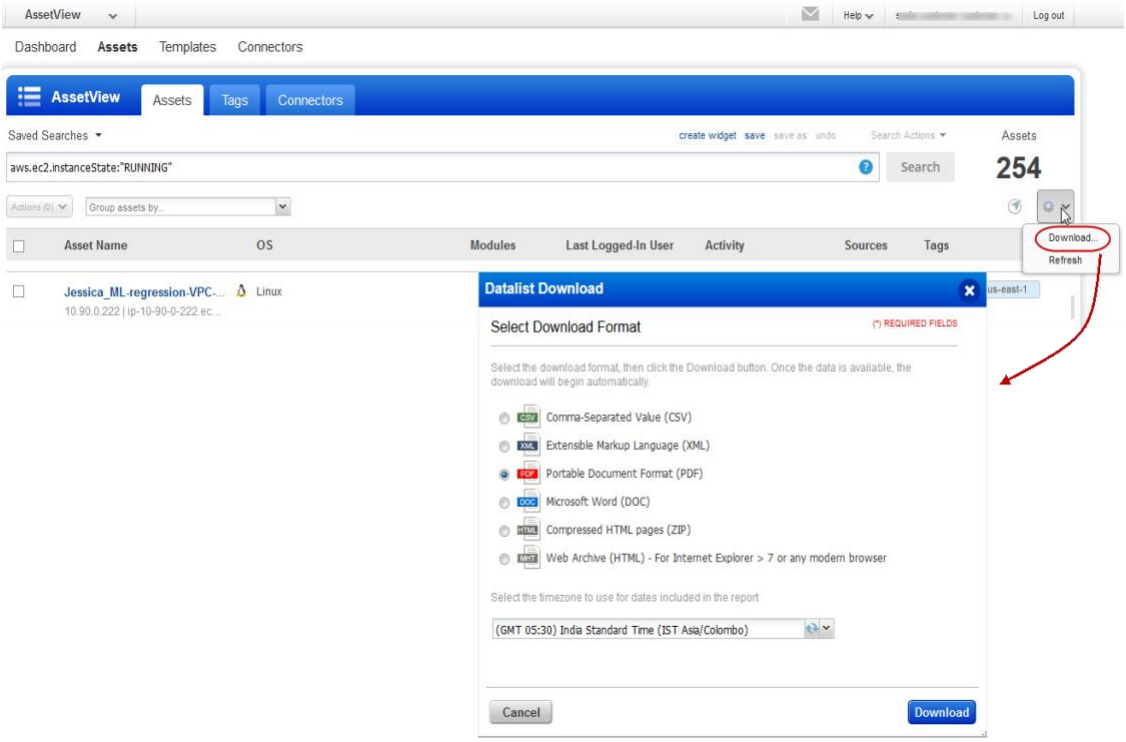
クエリの保存

検索を簡単に保存して再利用し、他のユーザーと共有できます。



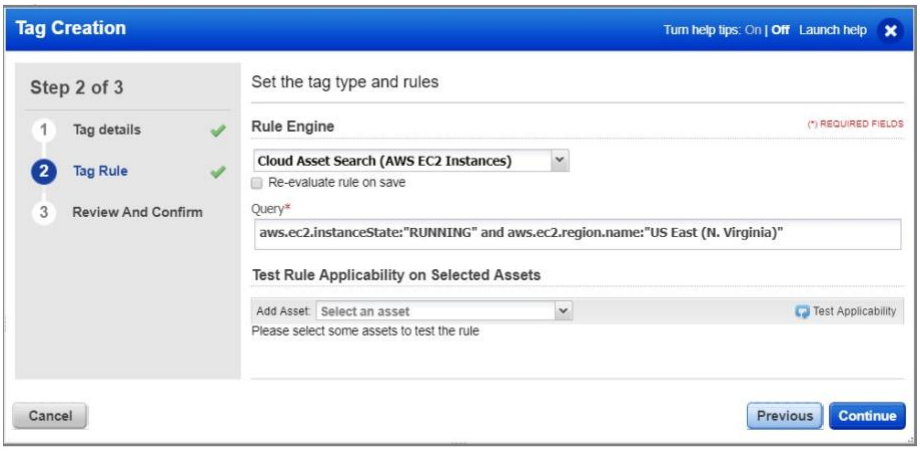
結果のダウンロードとエクスポート

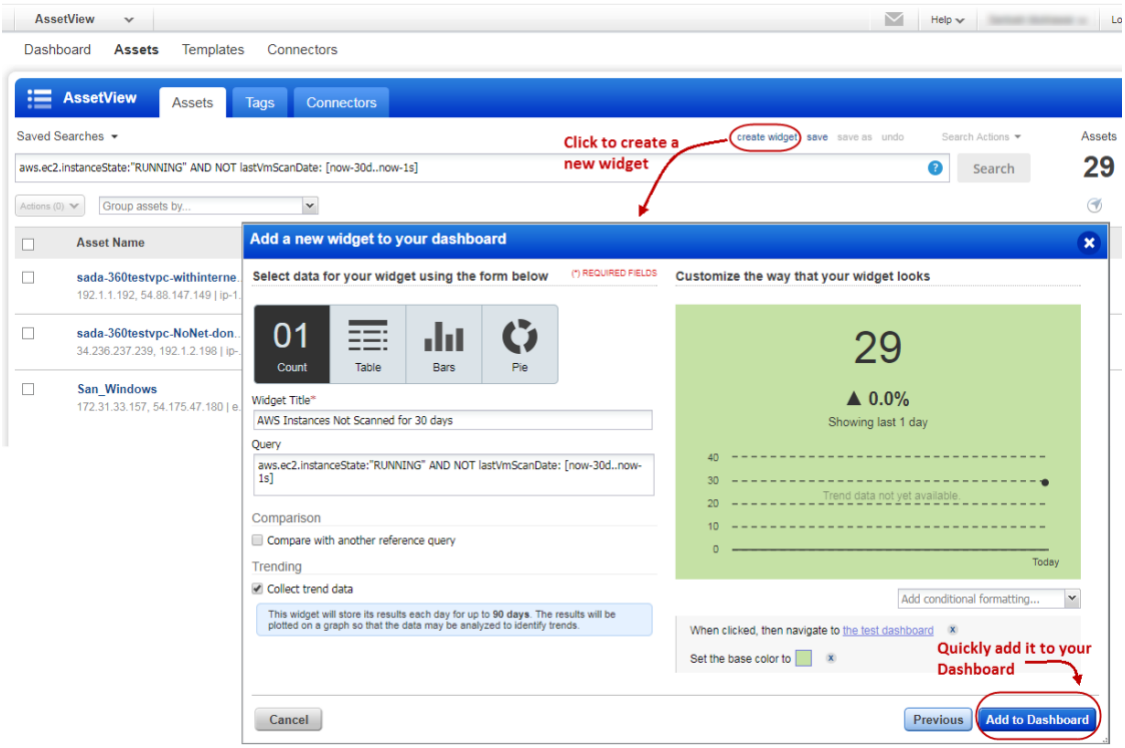
検索結果のエクスポートには数分しかかかりません。「ツール」メニューから「ダウンロード」を選択します。次に、エクスポート形式を選択し、[ダウンロード]をクリックします。結果は複数の形式(CSV、XML、PDF、DOC、HTML など)でエクスポートできます。



ウィジェットを作成

アセットのクエリを実行してウィジェットを作成し、ダッシュボードに追加します。たとえば、実行状態で 1 か月間スキャンされていない AWS アセットを検索します。クエリを入力し、[ウィジェットの作成] をクリックします。次に、ウィジェットをダッシュボードに追加します。





EC2 属性を使用した動的タグ付け

EC2 コネクタによって収集されたアセットの EC2 メタデータ属性を使用して、動的タグを作成します。次に、EC2 スキャンのスコープとして動的タグを使用します。AssetView >に移動

アセット>タグ] をクリックし、Cloud Asset Search (AWS EC2 インスタンス) タグルールを使用してタグを作成します。

レポートの生成

EC2 アセットの脆弱性を特定するためのレポートを作成できます。[レポート] > [レポート] > [新しい>スキャンレポート] に移動するだけです。次に、事前設定されたテンプレートまたはカスタマイズされたテンプレートを選択できます。

レポートにタイトルを付け、テンプレート、レポート形式、ホスト(IP アドレスまたはタグ)を選択して、レポートを生成します。

テンプレートのカスタマイズに応じて、レポートには、脆弱性情報を示すグラフやチャート、およびイメージ ID、VPC ID、インスタンスの状態、タイプなどの EC2 インスタンス情報が含まれる場合があります。インスタンス情報を修復に使用し、ホストの脆弱性を修正できます。

以下は、EC2 アセットに関するレポートのサンプルです。

10.90.0.188 (i-a5d043c0, i-a5d043c0, IP-0A5A00BC) Windows 2008 Service Pack 2
CRM-27891Net

Host Identification Information
IPs
Asset Id

EC2 related Information	
Public DNS Name	
Image Id	ami-c91ccba0
VPC Id	vpc-1e37cd76
Instance State	RUNNING
Private DNS Name	ip-10-90-0-188.ec2.internal
Instance Type	m1.medium

Associated Tags: CRM-27891, QCon1, Set1, TagPOR7098, set4;

Vulnerabilities Total	10 (0) -	Security Risk	3.1

by Status			
Status	Confirmed	Potential	Total
New	0	-	0
Active	10	-	10
Re-Opened	0	-	0
Total	10	-	10
Fixed	0	-	0
Changed	0	-	0

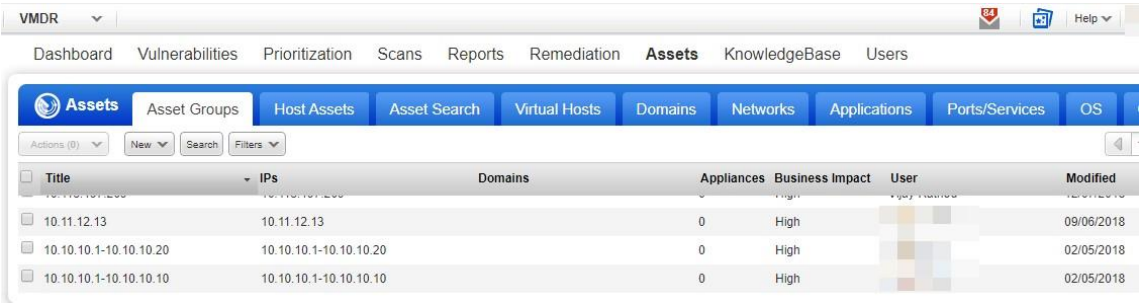
Qualys を使用したアセットの管理

ここでは、Qualys を使用して AWS EC2 インフラストラクチャを保護するのに役立つアセットを整理するためのベストプラクティスとヒントをいくつか紹介します。

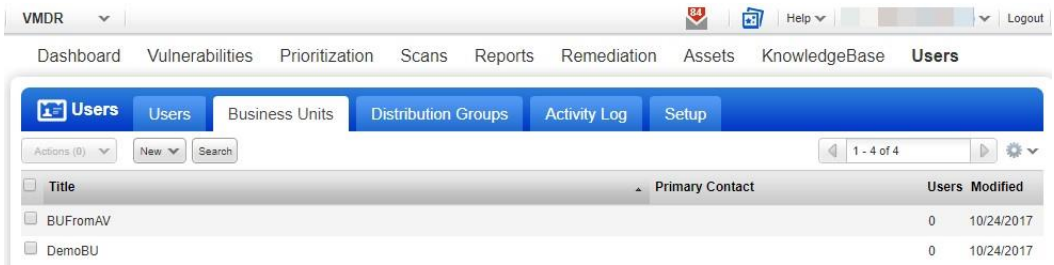
Qualys 構成のセットアップ

アセットグループ - アセットを意味のあるグループに整理し、サブユーザーに割り当てます。

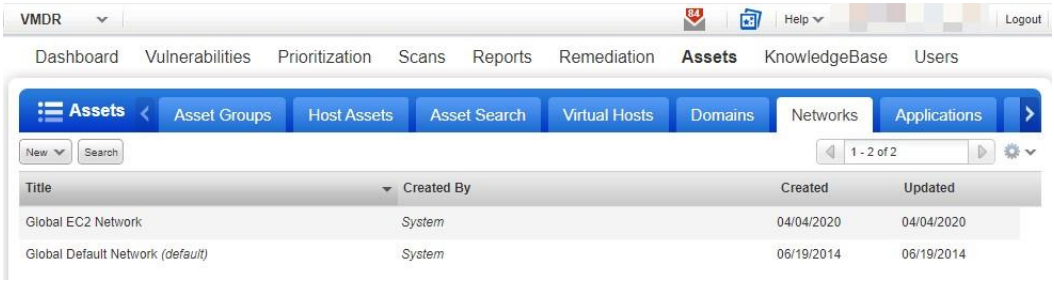
アセットグループは、スキャナー、リーダー、ユニットマネージャー(ビジネスユニットが定義されている場合)など、複数のユーザーがいる場合に必要です。同じ IP アドレスを複数のアセットグループに含めることができます。



Business Units - 組織に合った方法で、ユーザーとアセットを Business Units に整理します。これにより、マネージャーは、割り当てられた Business Units のコンテキストでロールベースの権限をユーザーに付与できます。同じ IP アドレスを複数の Business Units に含めることができます。

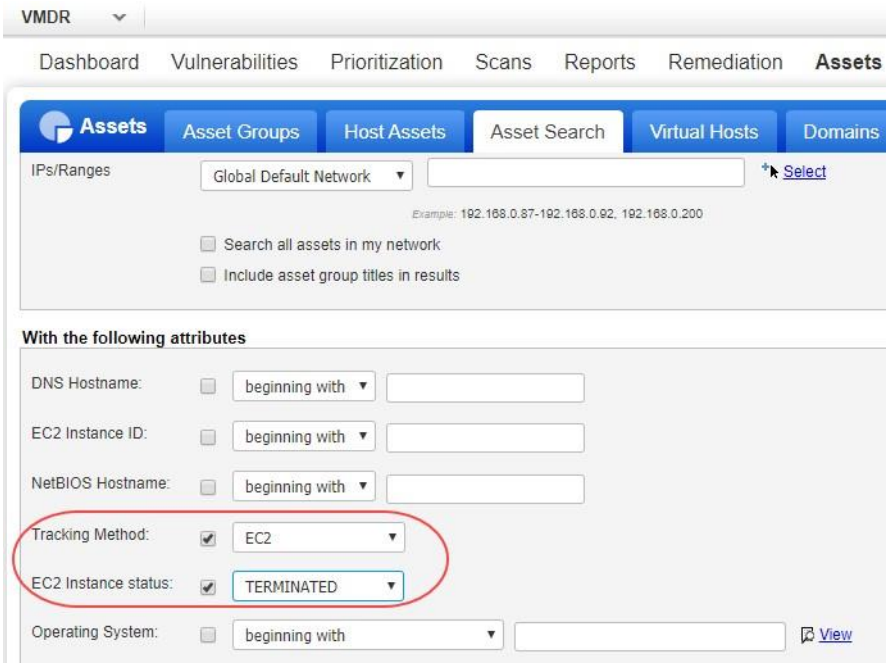


ネットワーク - 個別のプライベート IP ネットワークを編成して、重複する IP ブロックを分離します。設定すると、Qualys はネットワークと IP アドレスで IP を追跡します。留意点 IP アドレスは、サブスクリプションまたは 1 つのネットワークに対して一意である必要があります。

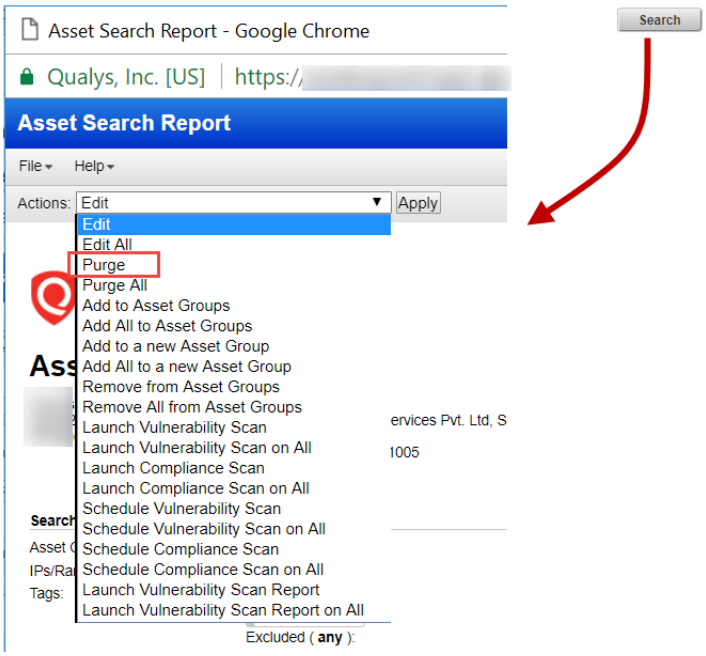


終了したインスタンスの削除 – Qualys のアカウントからインスタンスを終了できます。

[Asset Search] > [Vulnerabilities Management] または [Policy Compliance > Hosts Hosts] に移動し、追跡方法が EC2 のアセットを選択します。また、パラメーターを追加して、たとえば x 日以内ではない最終スキャン データなどを絞り込むこともできます。



「検索」をクリックし、「アクション」メニューから「パージ」を選択します。これにより、アセットとその関連データがモジュールから削除されます。



EC2 アセットにクラウドエージェントをデプロイし、過去 N 日間チェックインされていないエージェントをアンインストールするシナリオを考えて、API 呼び出しを使用できます。

リクエスト：

```
curl -u "USERNAME:PASSWORD" -X "POST" -H "Content-Type: text/xml"
-H
"Cache-Control: no-cache" --data-binary
@uninstall_agents_not_checkedin.xml
"https://qualysapi.qualys.com/qps/rest/2.0/uninstall/am/asset/"
```

Contents of uninstall_agents_not_checkedin.xml:

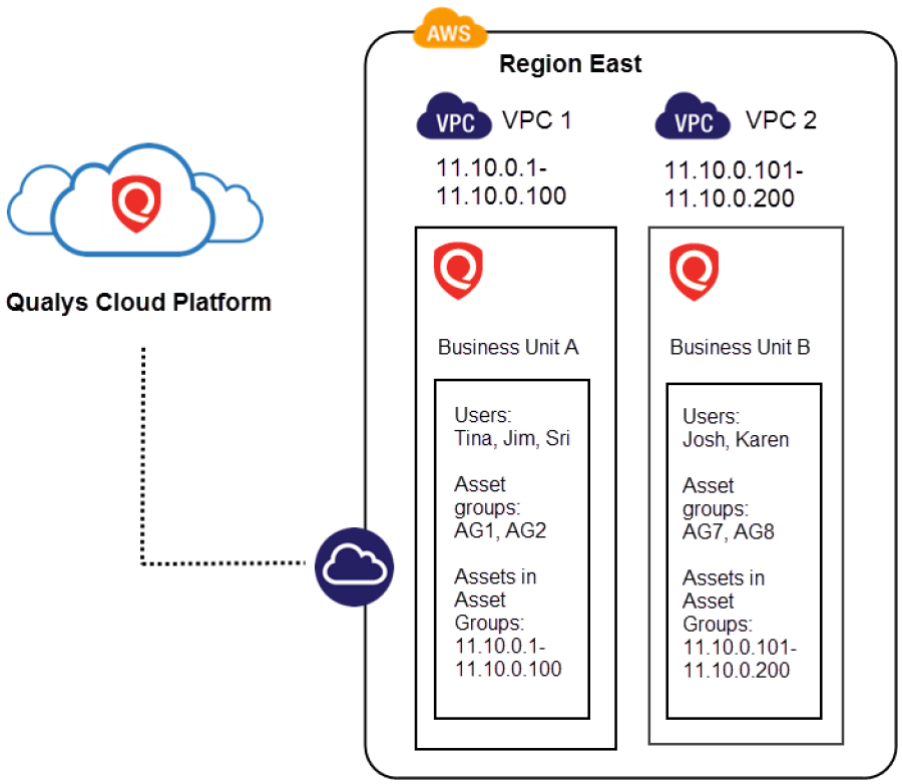
```
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
<filters>
<Criteria field="tagName" operator="EQUALS">Cloud Agent</Criteria>
<Criteria field="updated" operator="LESSER">2016-08-
25T00:00:01Z</Criteria>
</filters>
</ServiceRequest>
```

Cloud Agent APIの詳細については、Cloud Agent APIユーザーガイドを参照してください。

AWS 環境をスキャンするためのユースケース

ユースケース 1 - IP が重複しない複数の VPC のスキャン

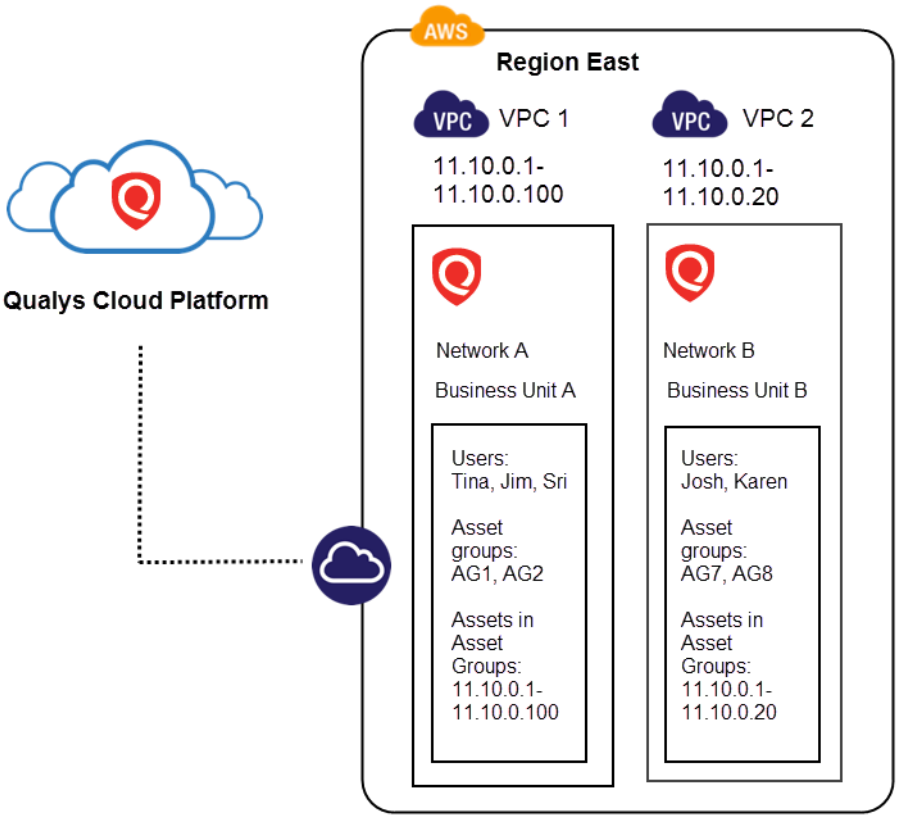
- アセットグループを定義する必要があり、ビジネスユニットはオプションです
- ビジネスユニットを定義すると、自分のビジネスユニット内のアセットへのユーザーアクセスが制限されます。Business Units A のユーザーは、Business Units B のアセットにアクセスできません。
- グループ AG1、AG2、AG7、AG8 に重複する IP アドレスがない場合の解決策。



ユースケース 2 - IP が重複する複数の VPC のスキャン

- ネットワーク、ビジネスユニット、アセットグループを定義する必要がある
- ビジネスユニットは、自分のビジネスユニット内のアセットへのユーザーアクセスを制限します。Business Units A のユーザーは、Business Units B のアセットにアクセスできません。
- ネットワーク A (アセット グループ AG1、AG2) とネットワーク B (AG7、AG8) に重複する IP アドレスがある場合のソリューション

注: ネットワークは、同じビジネスユニット内に配置することもできます。



DevOps セキュリティ

DevOps を統合し、スキャン自動化のプロセスを高速化できるさまざまな方法を見てみましょう。

Automate scanning into DevOps process to harden the AMI

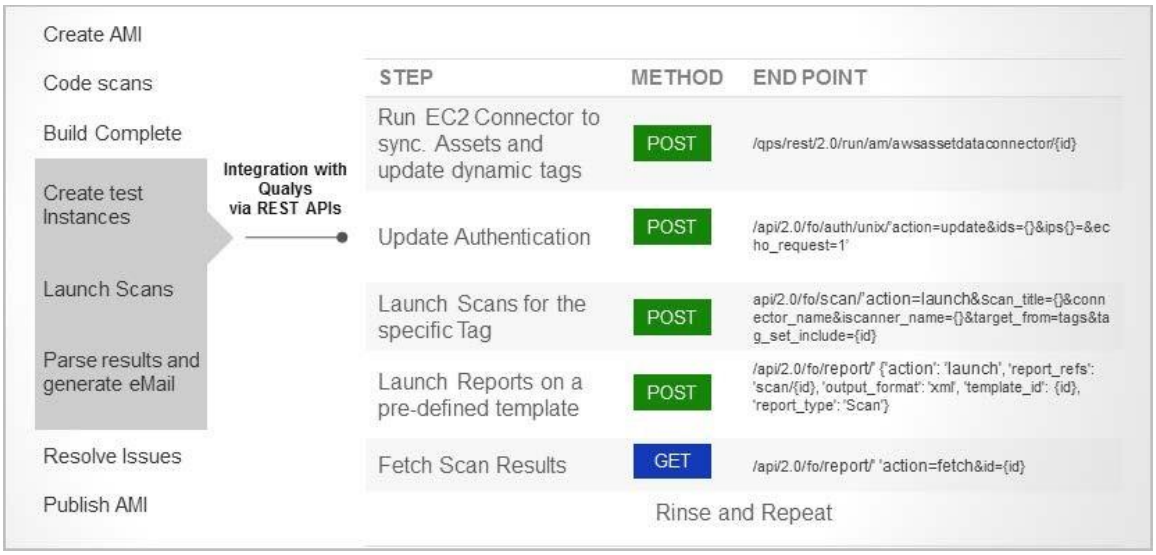
Automate VM scanning of host and EC2 cloud instance from Jenkins

Golden AMIs Pipeline

DevOps プロセスへのスキャンを自動化して AMI を強化

AWS では、公開されている AMI を使用して独自のカスタム Amazon マシンイメージ (AMI) を作成するのがベストプラクティスです。その後、事前設定された OS とソフトウェアをカスタマイズして、アプリケーションを実行できます。ただし、このようなカスタム AMI は、本番稼働ワークロードに使用する前に包括的にテストする必要があります。また、AMI に対して脆弱性スキャンを実行して、アプリケーションの脆弱性やベストプラクティスからの逸脱を評価する必要があります。Qualys は、AMI イメージをスキャンするための DevOps プロセスに統合するための、すぐに使用できる API を提供します。

たとえば、AMI の作成に関連する一般的な手順と、Qualys API を使用して AMI を強化する方法を次に示します。

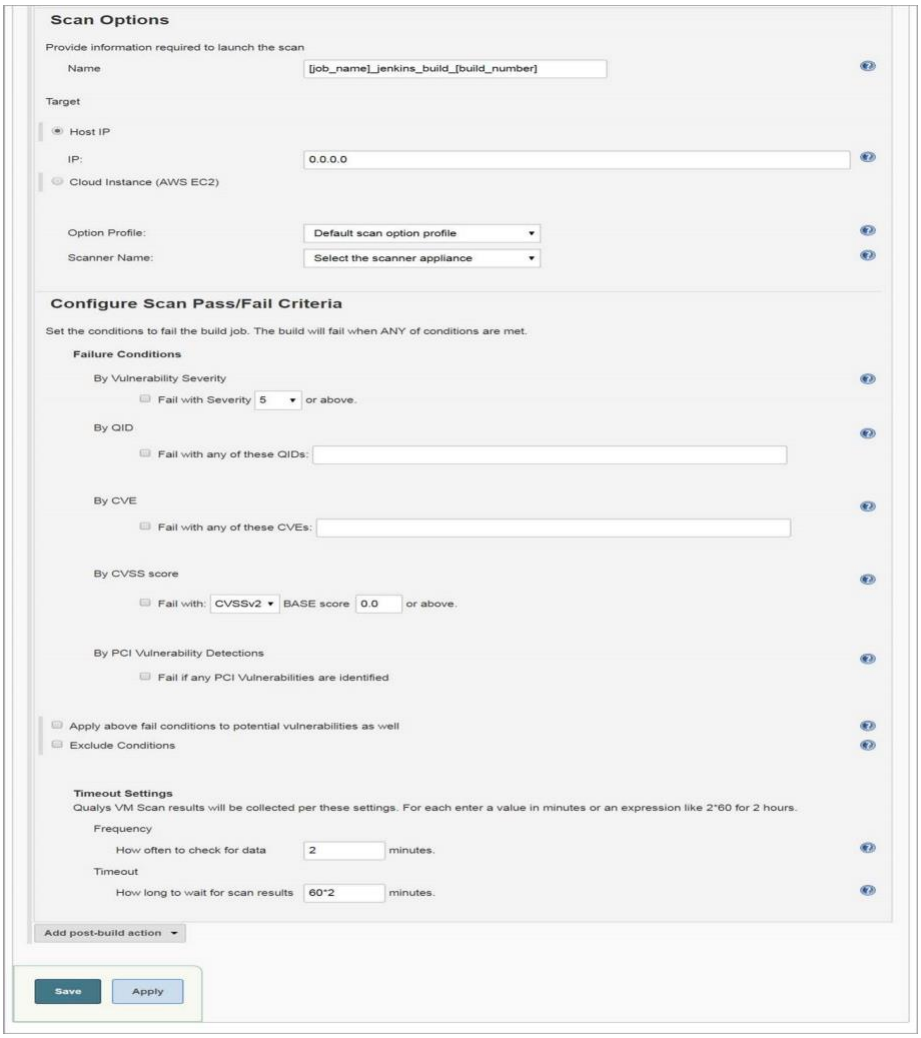


AWS に関連する Qualys API の使用の詳細については、『Asset Management and Tagging API v2 User Guide』を参照してください。

Jenkins からのホストと EC2 クラウドインスタンスの VM スキャンを自動化

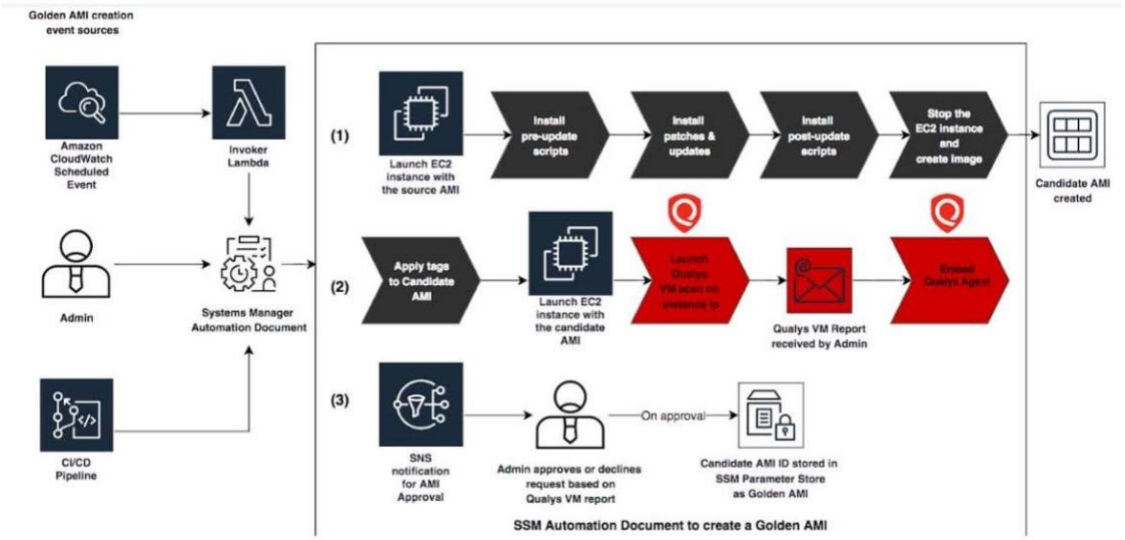
DevOps チームは、「Qualys VM Jenkins プラグイン」を使用して、Jenkins からホストと EC2 クラウドインスタンスの VM スキャンを自動化できます。この方法でスキャンを統合することで、ホストまたはクラウドインスタンスのセキュリティテストを行い、セキュリティ上の欠陥を検出して排除します。

「Jenkins Plugin for VM ユーザーガイド」を参照してください。



ゴールデン AMI パイプライン

ゴールデン Amazon マシンイメージ (AMI) を開発する場合、DevOps チームは継続的かつ自動化されたチェックを実行して、脆弱性や設定ミスを排除する必要があります。Qualys は Amazon と協力して、AWS Golden Amazon Machine Image Pipeline リファレンスアーキテクチャを Qualys スキャナーと統合し、AWS 環境に存在する強化された AMI のポートフォリオに対して継続的な評価を実行しました。これにより、イメージ作成パイプラインの重大な脆弱性とコンプライアンスの問題を、運用環境に到達する前に検出して修正できます。

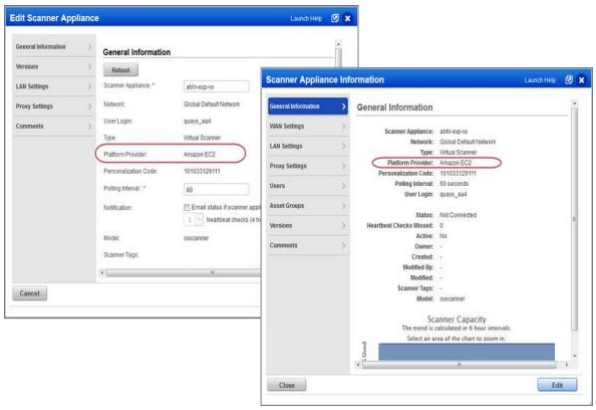


Qualys と Amazon のゴールデン AMI の統合の詳細については、参考資料「AWS ゴールデン AMI パイプライン」、ビデオシリーズを参照してください。

また、脆弱性評価のために Qualys スキャナーとのゴールデン AMI パイプラインの統合に使用できるスクリプトも提供しています。 詳細情報。

一般的な質問

質問	回答
スキャン結果と EC2 インスタンス ID	EC2 スキャン結果は、EC2 インスタンス ID によってインデックス化されます。このようにして、IP アドレスの変更が発生した場合でも、アセットを追跡し続けます。スキャン中に IP アドレスの変更が見つかった場合、スキャン結果が処理されると、スキャン結果、スキャンレポート、および AssetView アセットインベントリに新しい IP アドレスが表示されます。
EC2 スキャンジョブは、終了した EC2 インスタンスをどのように処理しますか?	Qualys VM/VMDR または Qualys PC から起動された EC2 スキャンから、ステータスが [終了] のすべての EC2 インスタンスを自動的に除外します。この方法では、停止した EC2 インスタンスのスキャンは行われません。オンデマンド EC2 スキャンを開始した後に表示される「EC2 スキャンプレビューの起動」には、スキャンジョブが Scanner Appliance に送信された後にフィルタリングが行われるため、終了したインスタンスが一覧表示されます。



EC2 スキャンにはどのようなユーザー権限が必要ですか?	マネージャとユニットマネージャは、Qualys ライセンスに従って、Qualys VM/VMDR および Qualys PC を使用して EC2 スキャンを開始、スケジュール、管理できます。 Qualys VM/VMDR - EC2 アセットの脆弱性スキャンを実行する - 仮想 Scanner Appliance(AMI インスタンス)の設定 - Qualys AssetView(AV)を使用した EC2 コネクタの作成/管理 Qualys PC - EC2 アセットのコンプライアンススキャンを実行する - 仮想 Scanner Appliance(AMI インスタンス)の設定 - Qualys AssetView (AV) Unit Manager 要件を使用して EC2 コネクタを作成/管理する: EC2 環境の IP は、アセットグループを介してマネージャーがユニットマネージャーのビジネスユニットに追加する必要があります。ユニットマネージャによって設定されたアプライアンスは、マネージャがユニットマネージャのビジネスユニットのアセットグループに追加する必要があります。

仮想スキャナ アプライアンスのプラットフォーム プロバイダー情報を表示するにはどうすればよいですか?	Qualys アカウント内の Amazon EC2 (または別のクラウド プラットフォーム) にデプロイされている仮想スキャナ アプライアンスのプラットフォーム プロバイダー情報が表示されます。 この情報は、アプライアンスを表示または編集するときに ([スキャン] > [アプライアンス] から) [一般情報] セクションに表示されます。

接続のトラブルシューティング	Q 接続のトラブルシューティング Qualys Scanner Appliance は、HTTPS 経由で Qualys Cloud Platform に定期的に接続する必要があります。アプライアンスが適切に機能するように、接続の問題を解決してください。 スキャナと Qualys Cloud Platform の間にネットワーク障害がある場合、「通信障害」メッセージが表示されます。 通信障害は、ローカル ネットワークがダウンした、何らかの理由でインターネット接続が失われた、スキャナと Qualys クラウド プラットフォーム間のネットワーク デバイスのいずれかがダウンした、のいずれかの理由が原因である可能性があります。 ネットワーク エラー メッセージは、Scanner Appliance が Qualys Cloud Platform に接続しようとして失敗したことを示します。 トラブルシューティングに役立つエラー コードと説明が表示されます。 エラーは、プロキシ サーバおよび

Qualys Cloud Platform との接続エラーに関連している可能性があります。

Qualys Cloud Platform は、Amazon EC2 システム コンソール上の接続チェックと全体的なパーソナライゼーション プロセスの結果をログに記録します。

「qualysguard.qualys.com に接続できません - 修正してください。」と表示された場合。 メッセージを受信するには、VPN ネットワーク ACL とセキュリティ グループでアウトバウンド HTTPS (TCP ポート 443) アクセスが許可されていることを確認してください。 プロキシ サーバを使用している場合は、スキャナがプロキシ サーバに到達できること、およびプロキシ サーバが Qualys クラウド プラットフォームにアクセスできることを確認してください。