Qualys を使用した Amazon Web Services のセキュリティ保護

2020 年 5 月 14 日

無断複写・転載を禁じます。2017-2020 年 クォリスジャパン株式会社

Qualys および Qualys ロゴは Qualys, Inc. の登録商標です。その他すべての商標は、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 5

Qualys について 5
Qualys サポート 5

はじめに 6

Qualys の統合されたセキュリティプラットフォーム 6
前提条件 8

自動アセットインベントリ 10

EC2 コネクタの設定 10
- EC2 コネクタのアカウント間ロール認証 10
- ARN 認証 10
- CloudFormation テンプレート 12
- EC2 リージョンの選択 14
- アセットのアクティブ化 14
- CloudView での AWS コネクタの有効化 15
- タグの割り当て 15

既存のコネクタのアカウント間ロールへのアップグレード 17
ベースアカウント認証の使用 18
- ベースアカウントの作成 18
- 既存のコネクタがベースアカウントを使用するよう更新 19

EC2 コネクタの動作 22
インポートしたアセットの表示 22
AWS メタデータ 23
- AssetView コネクタおよび Cloud Agent 23
- AssetView コネクタのみ 24
- QID - 370098 Amazon EC2 Linux インスタンスメタデータ 24

アセットを検出するために EC2 コネクタによって使用される AWS API 25
EC2 コネクタ用 Qualys API 26

AWS EC2 環境でのスキャン 27

センサの配置 38

事前認証済み Virtual Scanner Appliance の配置 38
- コストとライセンス 38
- スキャナ配置の推奨事項 39
- 必要事項 40
- スキャナの配置 40
- Qualys プライベートクラウドプラットフォームのサポート 45

Qualys Cloud Agent の配置 46

アセットのスキャン 47
EC2 スキャンのチェックリスト 47
事前認証済み Virtual Scanner Appliance を使用したスキャン 53
EC2 スキャンのワークフロー 53
EC2 Classic インスタンスのスキャン 55
VPC インスタンスのスキャン 55
VPC ピアリング接続を使用したインスタンスのスキャン 55
GovCloud にある EC2 インスタンスのスキャン 56
Qualys Cloud Agent を使用した内部ネットワークのスキャン 57
Qualys スキャナを使用したペリミタースキャン 58
Web アプリケーションのセキュリティ保護 65

分析、レポート、改善 66
EC2 アセットをクエリする方法 66
EC2 属性を使用した動的タグ付け 68
レポートの生成 69

Qualys を使用したアセット管理 70
Qualys の設定 70
AWS 環境スキャンの使用例 73
使用例 1 - IP の重複のない複数 VPC のスキャン 73
使用例 2 - IP の重複のある複数 VPC のスキャン 74

DevOps セキュリティ 75
スキャン自動化を DevOps プロセスに統合して AMI を堅牢化 75
Jenkins からホストおよび EC2 クラウドインスタンスの VM スキャンを自動化 76
Golden AMI Pipeline 77

よくある質問 78

本書について

Qualys クラウドプラットフォームおよびクラウドのセキュリティスキャンへようこそ。本書では、Qualys クラウドセキュリティプラットフォームを使用して、クラウド IT インフラストラクチャをスキャンする Qualys ソリューションについて詳しく説明します。

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。詳細については、www.qualys.com をご覧ください。

Qualys サポート

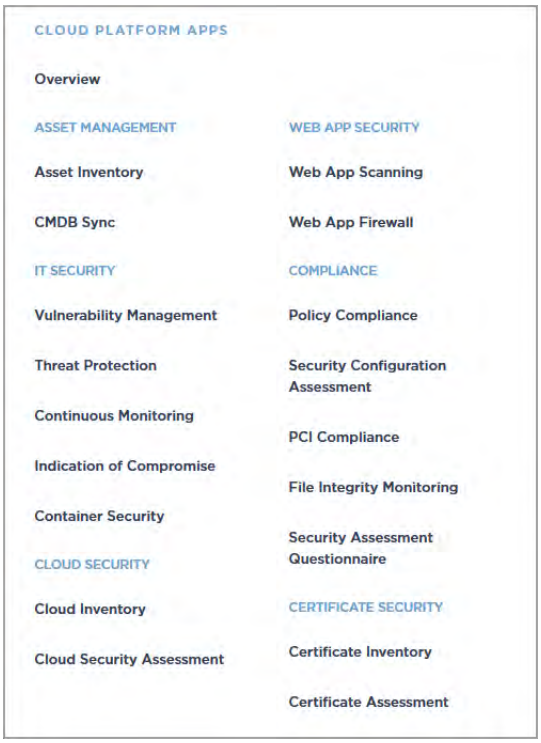
Qualys は綿密なサポートを提供します。不明な点には、オンラインドキュメント、電話サポート、および E メールによる直接サポートを通じて、可能な限り迅速にお答えします。弊社は 24 時間年中無休でサポートを提供します。サポート情報については、www.qualys.com/support/ をご覧ください。

はじめに

Qualys クラウドプラットフォームへようこそ。Qualys クラウドプラットフォームは、従来の IT インフラストラクチャに加え、クラウド IT インフラストラクチャのセキュリティを確保するためのソリューションを実現します。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のセキュリティを確保する方法について説明します。

Qualys の統合されたセキュリティプラットフォーム

Qualys クラウドプラットフォームを使用すると、セキュリティとコンプライアンスをリアルタムで、1 つのビューにまとめることができます。Qualys を初めて使用されるお客様は、当社のクラウドプラットフォームについてより詳しく知っていただくために、Qualys クラウドプラットフォームの Web ページを参照してください。



Qualys の AWS サポート

Qualys による AWS クラウドのサポートには、以下の機能があります。

- EC2 インスタンス（IaaS）を脆弱性から保護し、OS とアプリケーション（データベース、ミドルウェア）のコンプライアンスを定期的にチェック

- Cloud Agent を使用してセキュリティを継続的に確保し、これを AMI に埋め込むことにより完全な可視化を達成

- 外部公開されている IP および URL の脆弱性を特定

- アプリケーションスキャンとファイアウォールのソリューションによりアプリケーションのセキュリティを保護

- 事前認証済み脆弱性スキャン

- GovCloud を含む AWS のすべてのグローバルリージョンをサポート

- Classic および VPC プラットフォームの EC2 インスタンスをサポート

- EC2 での動作が認定された Qualys Cloud Agent

Qualys センサ

Qualys クラウドプラットフォームの中核的なサービスである Qualys センサを使用すると、グローバルな企業全体に対してセキュリティを容易に拡張することができます。センサは、リモートからの配置と一元管理が可能であり、自己更新機能を備えています。センサにより、データが収集され、Qualys クラウドプラットフォームに自動的に送信されます。Qualys クラウドプラットフォームには、脅威を特定して脆弱性を除去するために、情報の分析と相関付けを継続的に行う計算処理能力が備わっています。

Virtual Scanner Appliance
ネットワーク（ホストとアプリケーション）を横断するリモートスキャン

アプリケーション : VM/VMDR、PC、SCA、WAS

Cloud Agent
継続的なセキュリティ表示と追加のセキュリティソリューションのプラットフォーム

アプリケーション : CA（必須）、VM、PC

AWS クラウドコネクタ
クラウドインスタンスとメタデータの同期

アプリケーション : VM、PC

インターネットスキャナ
ネットワーク境界と接する IP および URL のペリミタースキャン

アプリケーション : VM、PC、WAS

Web Application Firewall
侵入をアクティブに防御しアプリケーションを保護

アプリケーション : WAF

前提条件

Qualys のユーザアカウントで、以下のオプションが有効化されている必要があります。

- Qualys アプリケーション ：Vulnerability Management（VM/VMDR）、Policy Compliance（PC）または Security Configuration Assessment（SCA）、Cloud Agent（CA）、Web Application Scanning（WAS）、Web Application Firewall（WAF）

- Qualys の Amazon AWS EC2 スキャンオプションが有効化されている必要があります。このオプションを使用できない場合は、Qualys の営業担当（TAM）またはサポートにお問い合わせください。

- Qualys センサ： Virtual Scanner Appliance、Cloud Agent（必要に応じて）

- マネージャまたはユニットマネージャのロール

始める前に

Qualys クラウドスイートの機能とインタフェースについて、すでにご存知かもしれませんが、初めて Qualys を使用される場合は、次の概要のチュートリアルを参照することをお勧めします（数分程度で済みます）。

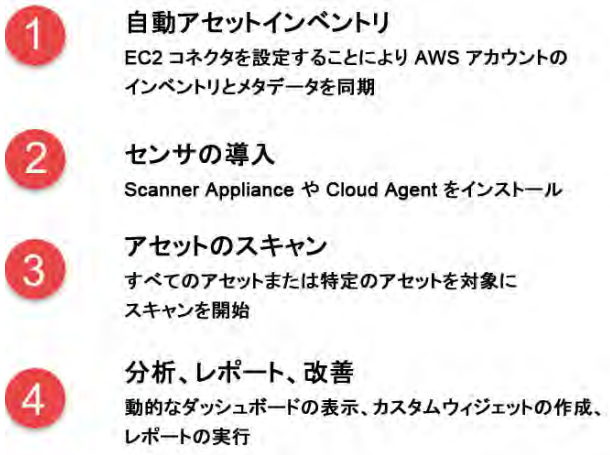
基本事項についての**ビデオチュートリアル**

脆弱性管理、検知および対応（約 3 分、英語）

ポリシーコンプライアンスの概要（約 14 分、英語）

クイックステップ : AWS のセキュリティ保護

Qualys を使用して AWS EC2 をセキュリティ保護するためのフローは以下のようになります。



役に立つリソース : 情報は最新の状態に保たれています

Qualys コミュニティ情報

Qualys トレーニング | 無料の自習用授業、ビデオシリーズ、オンラインコース（英語）

Qualys ドキュメント | 操作ガイド、クイック参照、API ドキュメント

Qualys AWS EC2 ビデオシリーズ | AWS アセットを検出して保護する方法を学習

自動アセットインベントリ

Amazon 用のコネクタは、Amazon API 統合を使用して、Amazon EC2 と VPC アセットを継続的に検出します。コネクタは 1 つまたは複数の Amazon アカウントに接続するように設定されているため、すべての Amazon EC2 リージョンと Amazon VPC における仮想マシンインスタンスインベントリに対する変更を自動的に検出して同期することができます。

AWS インスタンスは、時間の経過に伴って IP アドレスが変更されても、それぞれの Amazon インスタンス ID によって Qualys 内で追跡されます。Qualys のポリシーとレポート全体を駆動する、または影響を与えるアセットタグが、インポート処理の一環としてアセットエントリに自動的に割り当てられます。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、アセットの動的タグ付けをさらに実行するためのデータポイントとして Qualys に取り込まれて使用可能になります。

EC2 インスタンスの場合は、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。

EC2 コネクタの設定

これは、AWS インフラストラクチャのセキュリティを保護するための第一歩です。この項では、EC2 コネクタの設定に必要な手順について説明します。Qualys は、AWS アカウントごとに 1 つの EC2 コネクタを設定することをお勧めします。

アセットインベントリの検出と同期は、4 時間ごとに実行されます。アセットインベントリは、スキャンとは独立しています。「アセットを検出するために EC2 コネクタによって使用される AWS API」を参照してください。

EC2 コネクタのアカウント間ロール認証

アカウント間ロールを使用すると、Qualys は、AWS のセキュリティ資格情報を共有することなく AWS EC2 インスタンスにアクセスすることができます。Qualys は、AWS アカウントに作成された IAM ロールで AWS EC2 インスタンスにアクセスします。これにより、Qualys サブスクリプション内で IAM ユーザ鍵を管理することによるオーバーヘッドが削減されます。

ARN 認証

アカウント間ロール認証を使用して、新規の EC2 コネクタを作成することができます。アカウント間ロール認証を使用して EC2 コネクタを作成するステップを以下に示します。

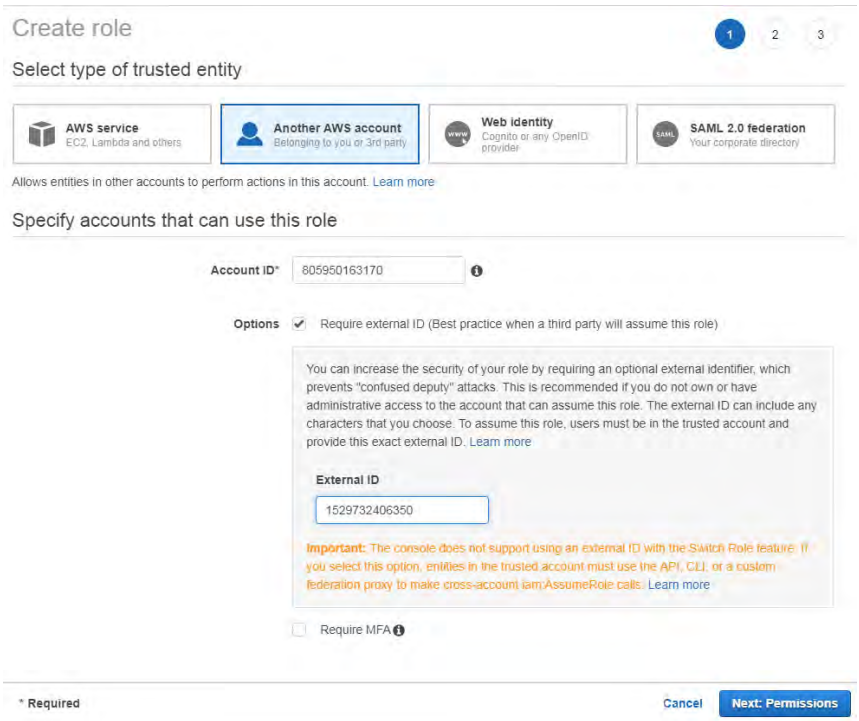
1）「AssetView（AV）」→「コネクタ」を選択し、「EC2 コネクタの作成」をクリックします。

2）コネクタ名と説明（オプション）を入力し、アカウントタイプを選択します。

3）AWS Console を開始し、「IAM」→「Roles」項へ移動します。「Create Role」をクリックします。

4）別の AWS アカウントを追加します。

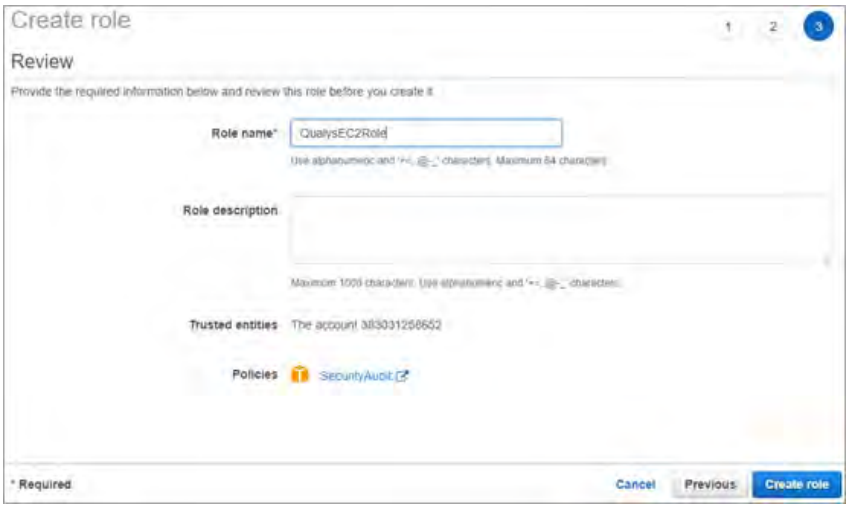
- ‘別の AWS アカウント’を選択します（コネクタごとに 1 つの AWS アカウントを使用します）。
- コネクタの詳細から「Account ID」（AWS アカウント ID）と「External ID」を貼り付けます。
- 「Next: Permissions」をクリックします。



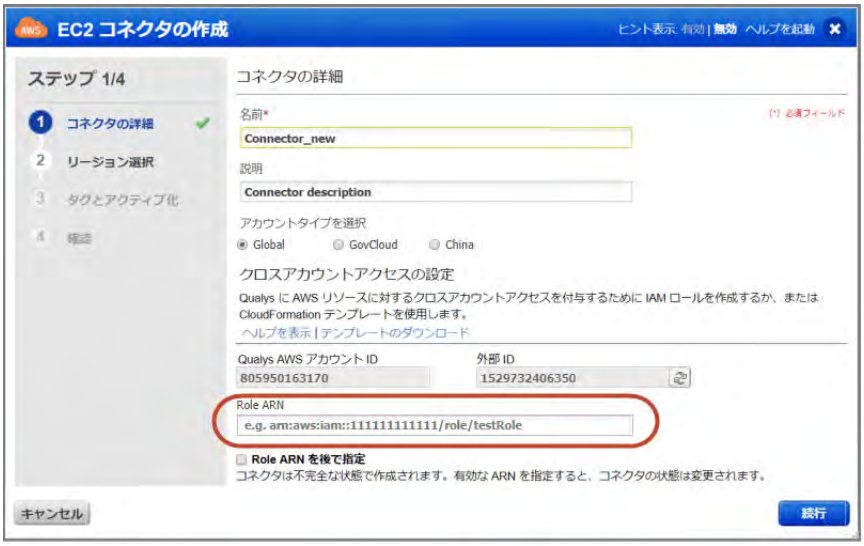
5)「SecurityAudit」というタイトルのポリシーを見つけ、横にあるチェックボックスを選択します。「Next: Tags」をクリックします。

6)「Next: Review」をクリックします。

7) ロールに名前（例 : QualysEC2Role）を入力し、「Create role」をクリックします。



8) 作成したロールをクリックして、詳細を表示します。「Role ARN」の値をコピーして、Qualys の「コネクタの詳細」に貼り付けます。



9) コネクタ作成のウィザードで「続行」をクリックして、残りのステップ（リージョン選択とタグとモジュールのアクティブ化）を完了します。

CloudFormation テンプレート

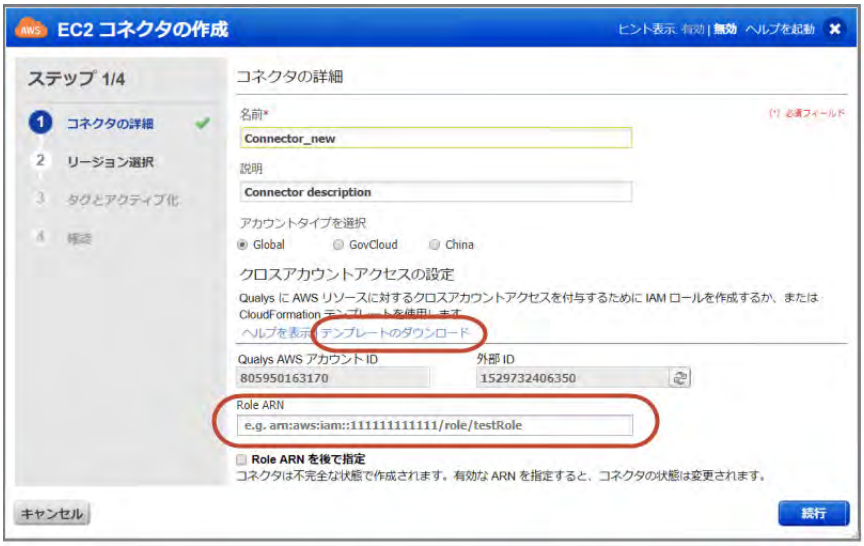
UI から直接ダウンロードすることのできる CloudFormation テンプレートを使用すると、EC2 コネクタの作成を自動化できます。

UI 手順に従って新規の EC2 コネクタを作成し、必要なロールを AWS Console で手動で作成するステップを示します。

1)「AssetView（AV）」→「コネクタ」を選択し、「EC2 コネクタの作成」をクリックします。

2）コネクタ名と説明（オプション）を入力し、アカウントタイプを選択します。

3)「テンプレートのダウンロード」リンクをクリックします。これにより、設定を行う AWS Console で実行可能な CloudFormation テンプレートがダウンロードされます。



4)「Role ARN を後で指定」オプションを選択します。これにより、コネクタが不完全な状態で作成されます。このコネクタは、後から ARN ロールを更新するために編集することができます。「続行」をクリックして残りのステップを実行し、コネクタの作成を終了します。

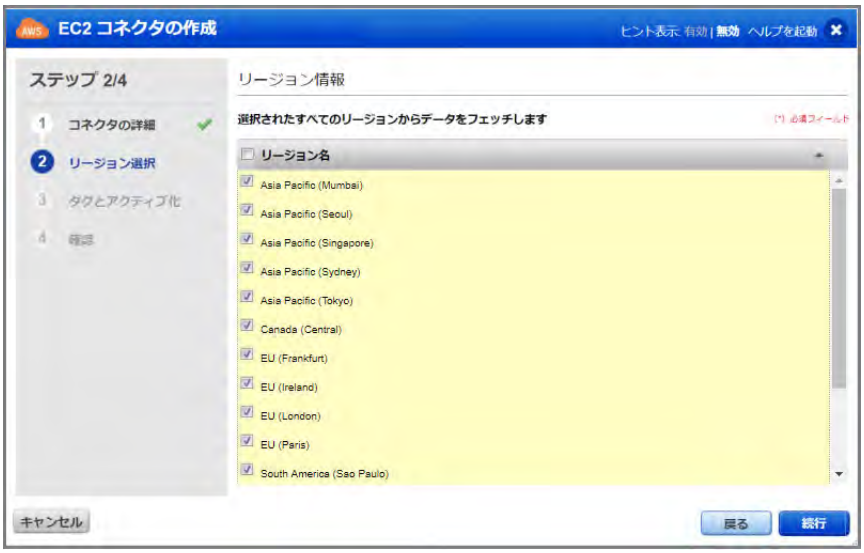
5）Amazon Web Services（AWS）にログインし、CloudFormation に移動します。

6）スタックを作成し、ステップ 3 でダウンロードしたテンプレートをアップロードします。スタックが完了したら、ARN ロールの値を出力からコピーします。

7)「AssetView（AV）」→「コネクタ」に戻り、フィルタを「不完全」状態に設定してコネクタを見つけます。コネクタを編集して、ARN の値を詳細に貼り付けます。

EC2 リージョンの選択

EC2 データを収集するリージョンを選択します。各リージョンのアセット数を取得するには、「アセットを同期」ボタンを使用します。少数のリージョンのみを選択した場合は、後から修正してリージョンを追加することができます。すべてのリージョンを選択することをお勧めします。こうすることで、誰かが別のリージョンでインスタンスを使用した場合でも表示されるようになります。



アセットのアクティブ化

EC2 アセットをスキャンするには、所有している Qualys ライセンスに対して EC2 アセットをアクティブ化する必要があります。事前認証済みのスキャナを AWS で使用する場合は、ここでアセットをアクティブ化する必要があります。そうでない場合は、AssetView から手動でアクティブ化します。「自動的にアクティブ化」を選択することにより、検出されたすべての EC2 アセット（サイズが中以上）がアクティブ化されます。これで、アセットをスキャンする準備が整いました。

アセットのタイプが m1.small、t1.micro または t2.nano のインスタンスはアクティブ化から除外されることに注意してください。このようなアセットは、Qualys にインポートはされますが、VM/VMDR、PC、または SCA に対してはアクティブ化されません。AWS で受け入れ可能なスキャンポリシーにより、m1.small、t1.micro、または t2.nano のインスタンスはスキャンできません。

アクティブ化を後から行う場合には、「AssetView」の「アセット」タブに移動してアクティブ化するアセットを選択し、「アクション」メニューから「アセットのアクティブ化」を選択します。

CloudView での AWS コネクタの有効化

AssetView で AWS コネクタを新規作成するか、既存のコネクタを編集するときに、「CloudView でコネクタ作成」オプションを使用すると、その AWS コネクタを CloudView アプリケーションでも使用できるようになります。これにより、CloudView で別途コネクタを作成する必要がなくなります。

AssetView でいったん有効にすると、後でこのオプションを無効にしても、対応するコネクタは CloudView から削除されません。CloudView アプリケーションからコネクタを明示的に削除する必要があります。

タグの割り当て

Qualys を使用した EC2 スキャンは、“ タグによるスキャン ” のワークフローに基づきます。Qualys のタグを EC2 のすべてのインスタンスに関連付けることがベストプラクティスです。事前認証済みのスキャンを使用してスキャンを行うには、タグの使用が必須になります。汎用のアセットタグ（例えば “ EC2 ”）を少なくとも 1 つ作成し、インポートしたすべてのアセットに対してこの EC2 タグを自動的に適用するようにコネクタを設定することをお勧めします。

検出された EC2 インスタンスの IP アドレスやその他の EC2 属性に基づいて動的にタグを作成し、このタグを EC2 アセットに自動的に適用することもできます。

コネクタの作成を終了するには、「完了」をクリックします。

次に実行すること

コネクタを作成したら、EC2 インスタンスを検出してアクティブ化し、Qualys アカウントに追加します。追加したアセットは、Qualys クラウドスイートアプリケーションのアセットインベントリに表示されます。

アプリケーション	アセットインベントリ
VM/VMDR、PC、SCA	「アセット」→「ホストアセット」タブ
AssetView	「アセット」タブ

既存のコネクタのアカウント間ロールへのアップグレード

アクセスキーを使用して作成した既存のコネクタを、アカウント間ロール認証を行うようにアップグレードすることができます。新しいコネクタではアカウント間のアクセルロールのみがサポートされ、アクセスキーベースのコネクタはサポートされません。

当社では、既存の EC2 コネクタからアカウント間アクセスロールを使用するコネクタへの移行を支援します。この既存の EC2 コネクタからアカウント間ロールへの移行は一方向であり、元に戻すことはできません。

アクセスキーベースのコネクタに対するサポートは、180 日後に停止されます。180 日以内に、アクセスキーベースのコネクタからアカウント間ロールにアップグレードしてください。

アクセスキーベースのコネクタからアカウント間ロールへアップグレードする手順

1)「AssetView」→「コネクタ」に移動します。アップグレードする EC2 コネクタを特定して右クリックし、「クイックアクション」メニューで「ARN ロールへアップグレード」を選択します。

ARN の詳細を入力し、「アップグレード」をクリックします。

同じ AWS アカウントにある複数の EC2 コネクタのアップグレード

一意の各 AWS アカウントに対して作成できるコネクタは 1 つに限られます。同じ AWS アカウントに対して複数の EC2 コネクタがある場合は、その中の 1 つのコネクタのみを保持する必要があります。コネクタを削除する前に、保持するアカウントに設定（リージョン、タグ、アクティブ化など）を追加したことを確認してから、アカウント間ロールベースの認証に切り替えてください。

同じ AWS アカウント内に重複しているコネクタがあり、その中の 1 つをアップグレードする場合は、重複しているコネクタを示す競合レポートが表示されます。

重複しているコネクタを削除してから、各 AWS アカウントで 1 つのコネクタのみが保持されるようにします。

> 一意の各 AWS アカウントに対して作成できるコネクタは 1 つに限られます。ARN にアップグレードする前に、重複しているコネクタを削除して複数の EC2 コネクタを 1 つにマージすることをお勧めします。

ベースアカウント認証の使用

アカウント間ロールを持つ 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たくない場合は、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。

Qualys アカウントを使用せずに AWS コネクタを設定する場合、自身の AWS アカウントをベースアカウントとして使用するよう設定できます。作成するベースアカウントに、AWS アカウント ID（複数の AWS アカウントがある場合は、少なくとも 1 つの AWS アカウント）を対応させる必要があります。

例えば、A1、A2、A3 の 3 つの AWS アカウントがあるとします。これらのアカウントのいずれか 1 つを選択して、ベースアカウントに対応させることができます。残りの 2 つのアカウントには、Qualys アカウントが使用されます。

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、同じアカウントタイプ（リージョン）でベースアカウントを作成します。ベースアカウントを作成しない場合でも、コネクタを作成できます。

「コネクタ」→「コネクタ」を選択し、「ベースアカウントの設定」をクリックします。名前、AWS アカウント ID、アクセスキー、および秘密鍵を指定してから、アカウントタイプを選択します。

作成できるベースアカウントは、アカウントタイプごとに 1 つのみになります。そのベースアカウントを設定する AWS アカウント ID に、AWS コンソールでポリシーが関連付けられていることを確認してください。AWS コンソールでの詳細な設定手順については、「AWS でのベースアカウント設定」を参照してください。

ベースアカウントの編集

編集するベースアカウントを選択し、「Quick action」メニューをクリックして「Edit」を選択します。アカウント名、AWS アカウント ID、アクセスキー、秘密鍵を編集できます。アカウントタイプは編集できません。

既存のコネクタがベースアカウントを使用するよう更新

アカウント間ロールを持つ既存の AWS コネクタがベースアカウントを使用するように更新するには、以下の手順を実行する必要があります。

- AWS アカウント ID を使用するベースアカウントを作成します（「ベースアカウントの作成」を参照してください）。

-「IAM Roles」の「Trust Entities」を更新します。AWS コンソールで、「IAM role」→「Trust relationships」を選択し、「Edit trust relationship」を選択します。そのベースアカウントを設定する AWS アカウント ID が、AWS コンソールの信頼できるリレーションシップのアカウント番号と一致することを確認します。「Update Trust Policy」をクリックします。

AWS でのベースアカウント設定

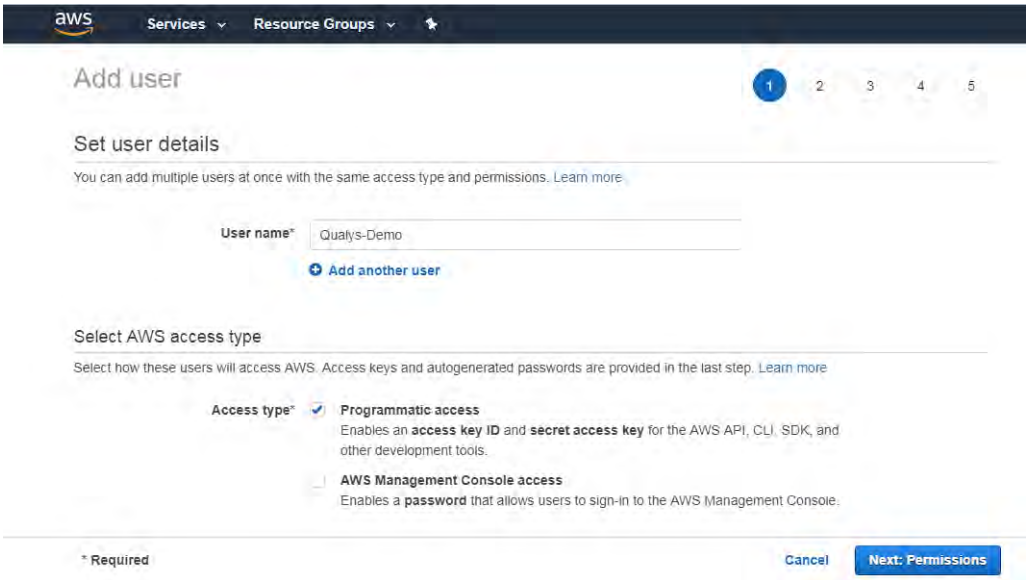
コネクタにベースアカウントを使用する場合、一定の前提条件と AWS コンソールで構成する必要のある設定があります。ベースアカウントを設定するために AWS コンソールで必要な手順と構成は以下のとおりです。

IAM ユーザの作成と AWS へのポリシーの関連付け

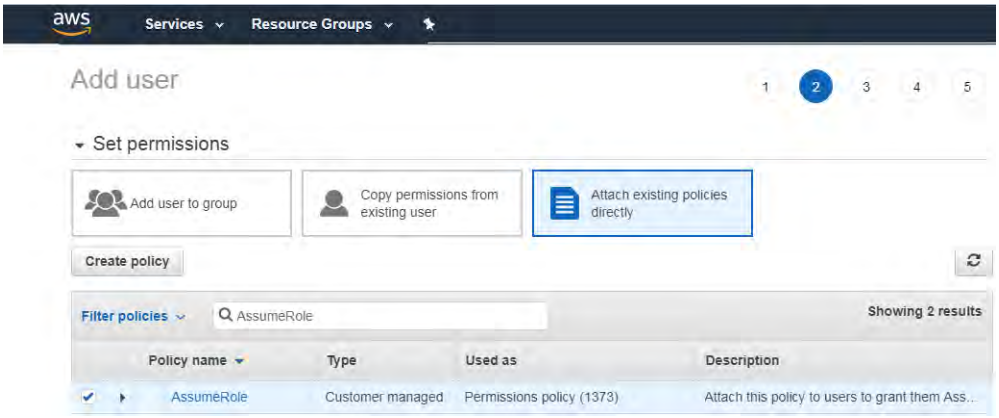
1. AWS コンソールで「AWS」→「Policies」を選択し、次の JSON コンテンツを含むポリシーを作成します（「AssumeRole」など）。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1501205548000",
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

2. IAM ユーザを作成します。「Identity and Access Management」→「Users」を選択し、「Add user」をクリックします。



3. ユーザ名を指定し、ユーザの「Programmatic access」を有効にします。「Next: Permissions」をクリックします。



4.「Attach existing policies directly」を選択し、「Filter policies」に作成したポリシーの名前（AssumeRole）を入力します。設定したポリシー（AssumeRole）を選択し、「Next: Tags」をクリックします。

必要に応じてタグを追加します（オプション）。設定したユーザ設定を確認し、「Create user」をクリックします。

EC2 コネクタの動作

アセット検出 : EC2 コネクタは、クラウド内から継続的な同期メカニズムを使用して、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も含む）を取得します。

AWS は、終了したインスタンスを 15 分間だけ保持します。ただし、Qualys には終了したすべてのインスタンスのレコードが保存されており、終了したインスタンスの履歴と詳細をいつでも追跡することができます。

アセットの同期 : Qualys アカウントにアセットを追加します。エラーのあるアセット（除外されたアセットなど）以外のすべてのアセットが Qualys アカウントに追加されます。

アクティブ化 : Scanner Appliance を使用したスキャンの実行を計画する場合は、Qualys アカウントに追加したアセットについて、Vulnerability Management/Policy Compliance/Security Configuration Assessment の各ライセンスをアクティブ化する必要があります。アクティブ化は手動で行うことも、EC2 コネクタの設定中に自動で行うこともできます。

アクティブ化からの除外 : アクティブ化から除外される終了したインスタンスの他に、m1.small、t1.micro、または t2.nano の各インスタンスもアクティブ化から除外されます。AWS で受け入れ可能なスキャンポリシーにより、m1.small、t1.micro、または t2.nano のインスタンスはスキャンできません。このようなインスタンスに対しては、Cloud Agent を使用することができます。

インポートしたアセットの表示

コネクタの作成が終了すると、EC2 コネクタはインスタンスの取得を開始します。コネクタの実行が完了したときに表示される各種の情報について説明します。

1. **アセット数** -「アセット数」カラムには 最後の EC2 コネクタの実行で検出および同期されたアセットの数が示されます。
2. **同期されたアセット** - 「アセット数」カラムの緑色の部分は、同期されたアセットを表します。同期されたアセット数は、Qualys で正常に処理されたアセットの数を示します。
3. **除外されたアセット** - 青色の部分は、同期されたが VM/PC/SCA のアクティブ化で除外されたアセットを表します。除外されたアセットは、終了したアセットであるか、または AWS のスキャンで受け入れ可能な使用ガイドにより Qualys スキャナではスキャンできない m1.small、t1.micro、または t2.nano である可能性があります。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. **表示アセット** – その期間にコネクタで検出されたアセットの総数です。

エラーのあるアセット - 「アセット数」カラムには、エラーのあるアセットを示す赤色の部分が示されることもあります。エラーのあるアセットとは、Qualys による処理中に問題が発生したアセットのことです。

コネクタによって収集されたアセットは、「AssetView」に移動すると表示されます。「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。次に示すのは、収集した情報を示すスクリーンショットの例です。

EC2 インスタンスの検出が完了すると、Amazon EC2 インフラストラクチャをスキャンしてセキュリティを確保する準備が整ったことになります。

AWS メタデータ

この項では、Qualys Cloud Agent、AssetView コネクタ、および Qualys Scanner が提供するクラウドプロバイダのメタデータに関する情報について説明します。

AssetView コネクタおよび Cloud Agent

General:

- Reservation ID

- Instance ID

- Instance Type

- Created Date

- Image (AMI) ID

- Account ID

- Instance State（QCA データ収集のための実行のみ）

Location:

- Region

- Availability Zone

- Zone

Network:

- 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 インスタンスメタデータ

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 コネクタによって使用される AWS API

Qualys では、EC2 インスタンスの検出と AWS アカウントからインスタンスについての追加情報を識別するために、次の 3 種類の API を使用します。これらの API の詳細については、下記の Amazon AWS の Web サイトを参照してください。

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_DescribeNetworkInterfaces.html

検出ジョブはオンデマンドで実行されるか、またはデフォルトの検出頻度（4 時間ごと）で実行されます。この頻度は、現在のところ変更できません。

EC2 コネクタ用 Qualys API

EC2 コネクタの各種の操作は、API 経由でも実行できます。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』（PDF、英語）を参照してください。

以下に便利な EC2 コネクタ API をいくつか示します。

AWS コネクタの作成

https://qualysapi.qualys.com/qps/rest/2.0/create/am/awsassetdataconnector

コネクタの実行

https://qualysapi.qualys.com/qps/rest/2.0/run/am/assetdataconnector/<id>

ホストのアセット情報の取得（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

まずネットワークの基本用語について説明します。

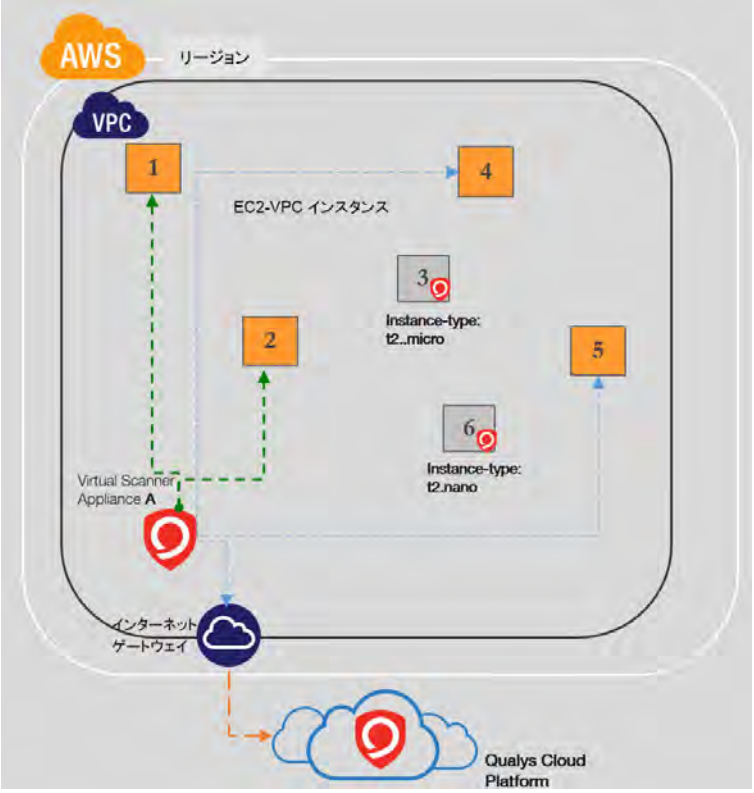
VPC: 定義した仮想ネットワーク内で AWS リソースを起動できます。これは、独自のデータセンターで運用する従来のネットワークとよく似ていますが、AWS のスケーラビリティを活用できるというメリットがあります。

VPC ピアリング接続: 2 つの VPC 間のトラフィックをルーティングできる、VPC 間ネットワーク接続です。

トランジットゲートウェイ： ネットワークトランジットハブです。これを使用して、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できます。

次に、AWS EC2 環境でスキャンを実行するためのさまざまなシナリオを紹介します。

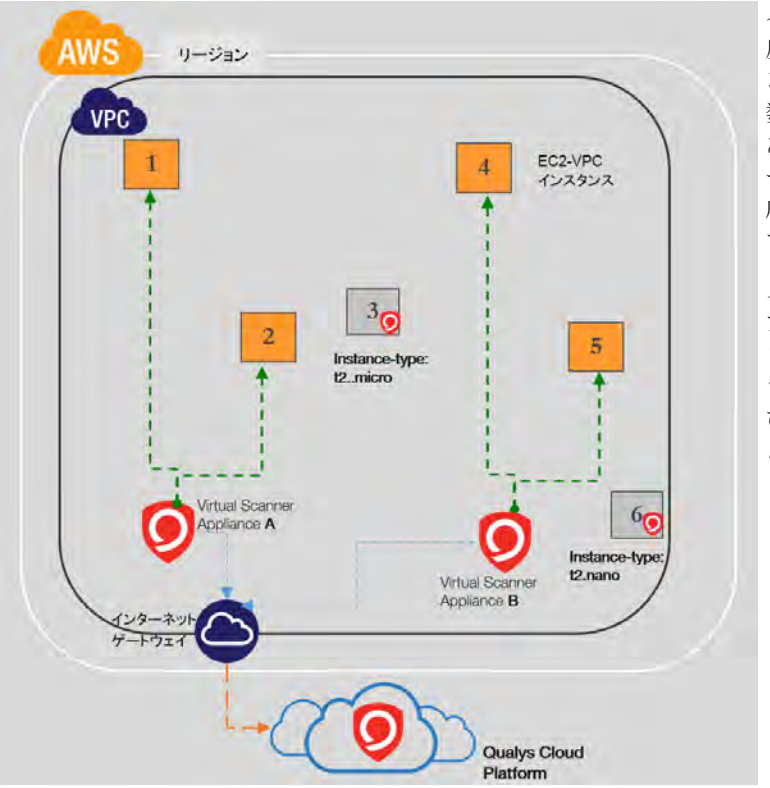
VPC 内で 1 つのスキャナが複数のインスタンスをスキャンする場合



スキャナが HTTPS 経由（セキュリティグループおよびインターネットゲートウェイ経由）で Qualys クラウドプラットフォームと AWS EC2 および STS エンドポイントに接続するよう、設定する必要があります。

AWS では、お使いの環境が中断される可能性を最小限にするために、セキュリティ評価から、EC2 インスタンスタイプの T3.nano、T2.nano、T1.micro、M1.small を除外することを推奨しています。これらをスキャンする場合は、Cloud Agent の使用を推奨します。

VPC 内で複数のスキャナが複数のインスタンスをスキャンする場合

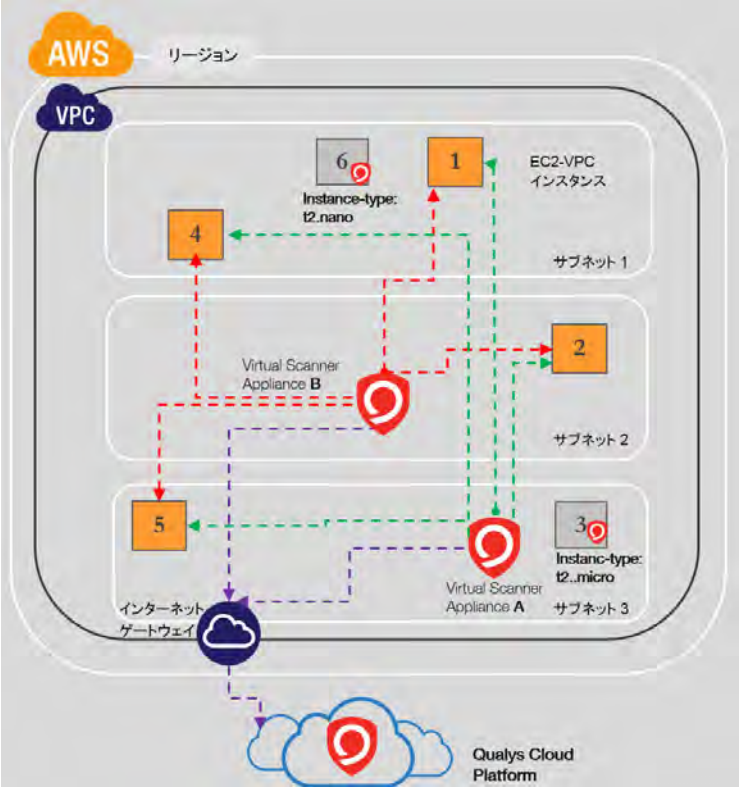


インスタンスの数とスキャンの頻度によっては、VPC 内で複数のインスタンスをスキャンするのに複数のスキャナが必要になる場合があります。各 VPC で少なくとも 1 つのスキャナが必要です。要件に応じて、さらにスキャナを追加してください。

スキャナが（セキュリティグループおよびインターネットゲートウェイ経由で）Qualys クラウドプラットフォームと AWS EC2 および STS エンドポイントに接続するよう、設定する必要があります。

AWS では、お使いの環境が中断される可能性を最小限にするために、セキュリティ評価から、EC2 インスタンスタイプの T3.nano、T2.nano、T1.micro、M1.small を除外することを推奨しています。これらをスキャンする場合は、Cloud Agent の使用を推奨します。

VPC 内のサブネット間で 1 つのスキャナが複数のインスタンスをスキャンする場合

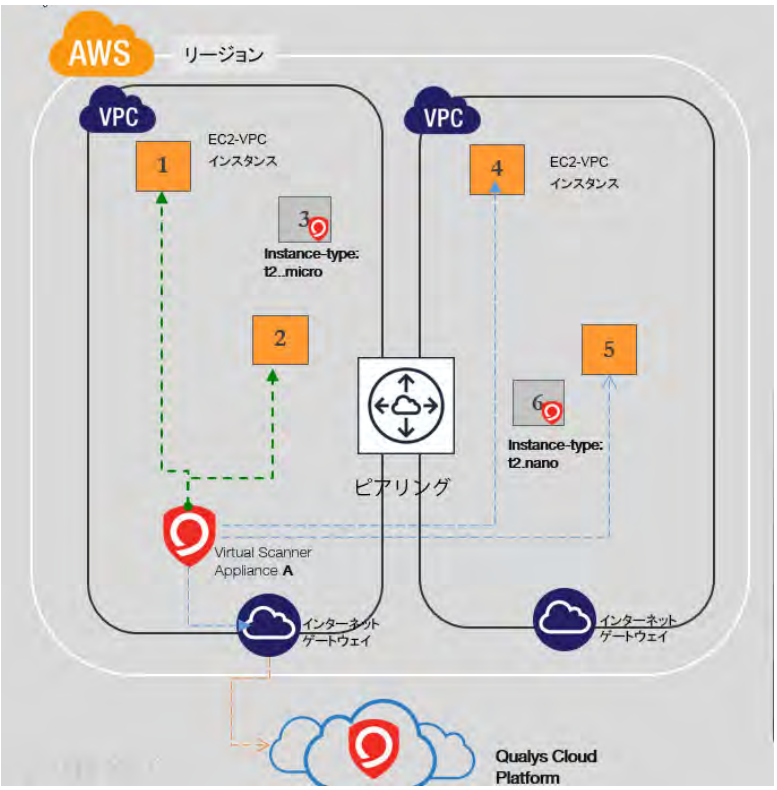


導入されているネットワークに制限がない限り、スキャナは通常、VPC 内のサブネット間で機能します。

スキャナが HTTPS 経由（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 Qualys クラウドプラットフォームおよび AWS EC2 および STS エンドポイントに接続するよう、設定する必要があります。

AWS では、お使いの環境が中断される可能性を最小限にするために、セキュリティ評価から、EC2 インスタンスタイプの T3.nano、T2.nano、T1.micro、M1.small を除外することを推奨しています。これらをスキャンする場合は、Cloud Agent の使用を推奨します。

リージョン内のピアリング接続された VPC 間で 1 つのスキャナが複数のインスタンスをスキャンする場合

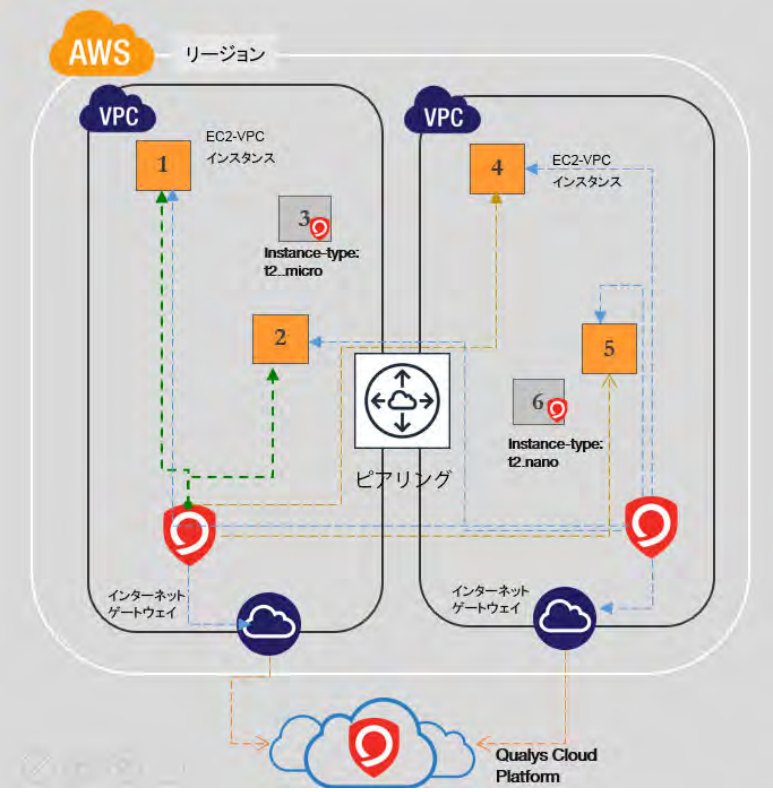


要件に応じて、さらにスキャナを追加してください。

スキャナが HTTPS 経由（セキュリティグループおよびインターネットゲートウェイ経由）で Qualys クラウドプラットフォームと AWS EC2 および STS エンドポイントに接続するよう、設定する必要があります。

AWS では、お使いの環境が中断される可能性を最小限にするために、セキュリティ評価から、EC2 インスタンスタイプの T3.nano、T2.nano、T1.micro、M1.small を除外することを推奨しています。これらをスキャンする場合は、Cloud Agent の使用を推奨します。

ピアリング接続された VPC 間で複数のインスタンスをスキャンするのに複数のスキャナが必要な場合

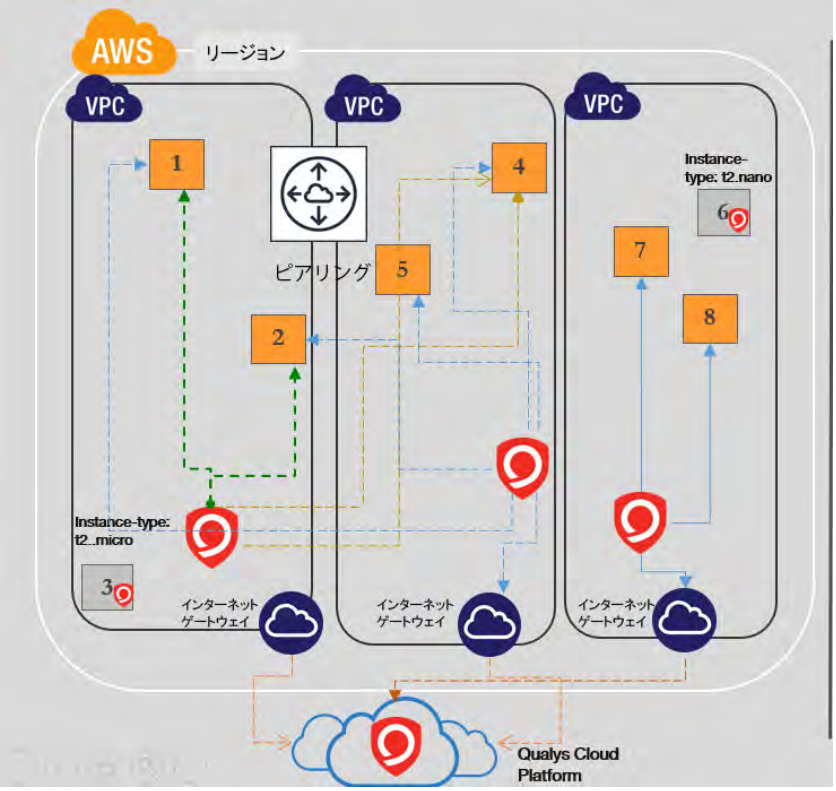


インスタンスの数とスキャンの頻度によっては、リージョン内のピアリング接続された VPC 間で複数のインスタンスをスキャンするのに複数のスキャナが必要になる場合があります。要件に応じてスキャナを追加し、VPC の境界を超えてスキャンができるようにしてください。

スキャナが HTTPS 経由（セキュリティグループおよびインターネットゲートウェイ経由）で Qualys クラウドプラットフォームと AWS EC2 および STS エンドポイントに接続するよう、設定する必要があります。

AWS では、お使いの環境が中断される可能性を最小限にするために、セキュリティ評価から、EC2 インスタンスタイプの T3.nano、T2.nano、T1.micro、M1.small を除外することを推奨しています。これらをスキャンする場合は、Cloud Agent の使用を推奨します。

ピアリング接続されていない VPC 内のインスタンスをスキャナがスキャンできない場合

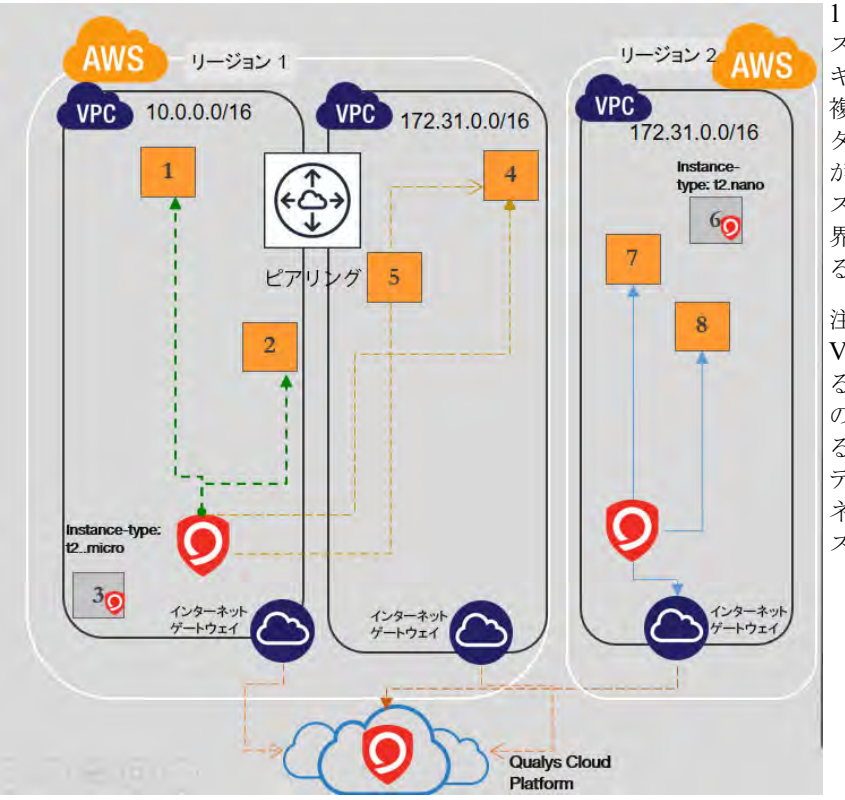


要件に応じてスキャナを追加し、VPC の境界を超えてスキャンができるようにしてください。

スキャナが HTTPS 経由（セキュリティグループおよびインターネットゲートウェイ経由）で Qualys クラウドプラットフォームと AWS EC2 および STS エンドポイントに接続するよう、設定する必要があります。

AWS では、お使いの環境が中断される可能性を最小限にするために、セキュリティ評価から、EC2 インスタンスタイプの T3.nano、T2.nano、T1.micro、M1.small を除外することを推奨しています。これらをスキャンする場合は、Cloud Agent の使用を推奨します。

IP アドレスが重複している VPC 内のインスタンスをスキャンできない場合



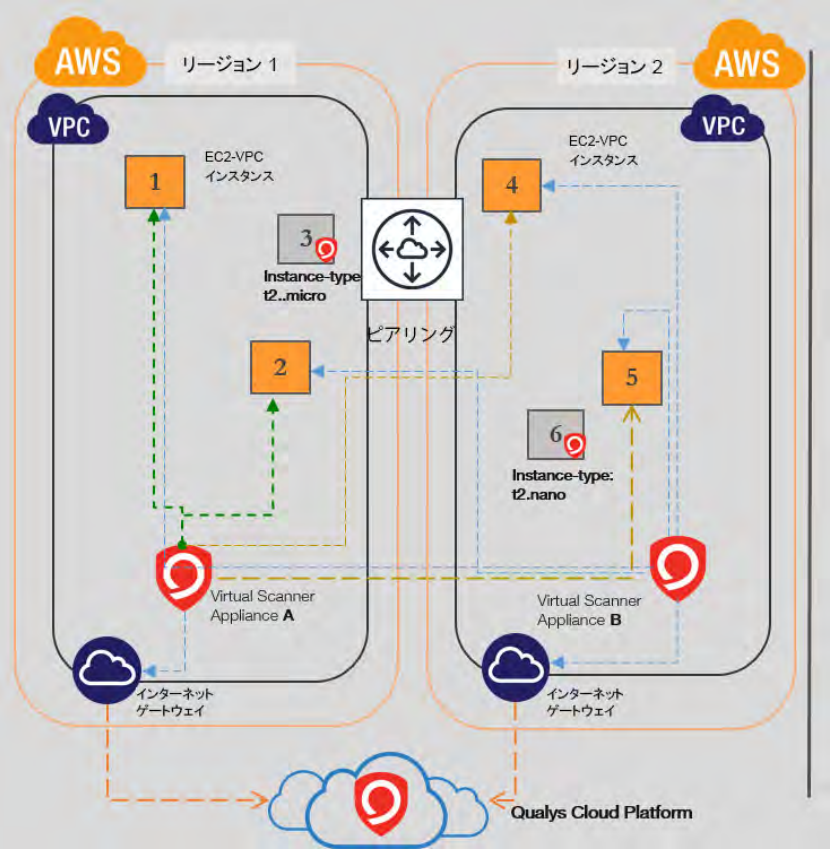
1 つのサブネットへのアクセス能力が原因で、1 つのスキャナでは、IP アドレスが重複している VPC 内のインスタンスをスキャンすることができません。要件に応じてスキャナを追加し、VPC の境界を超えてスキャンができるようにしてください。

注記：VPC の A と C 間で VPC ピアリングを設定できるにもかかわらず、B と C 間のサブネットが重複しているために、スキャナはルートテーブルに基づいてサブネットの 1 つのみにアクセスします。

スキャナが HTTPS 経由（セキュリティグループおよびインターネットゲートウェイ経由）で Qualys クラウドプラットフォームと AWS EC2 および STS エンドポイントに接続するよう、設定する必要があります。

AWS では、お使いの環境が中断される可能性を最小限にするために、セキュリティ評価から、EC2 インスタンスタイプの T3.nano、T2.nano、T1.micro、M1.small を除外することを推奨しています。これらをスキャンする場合は、Cloud Agent の使用を推奨します。

複数のリージョン内のピアリング接続された VPC 間で 1 つのスキャナが複数のインスタンスをスキャンする場合

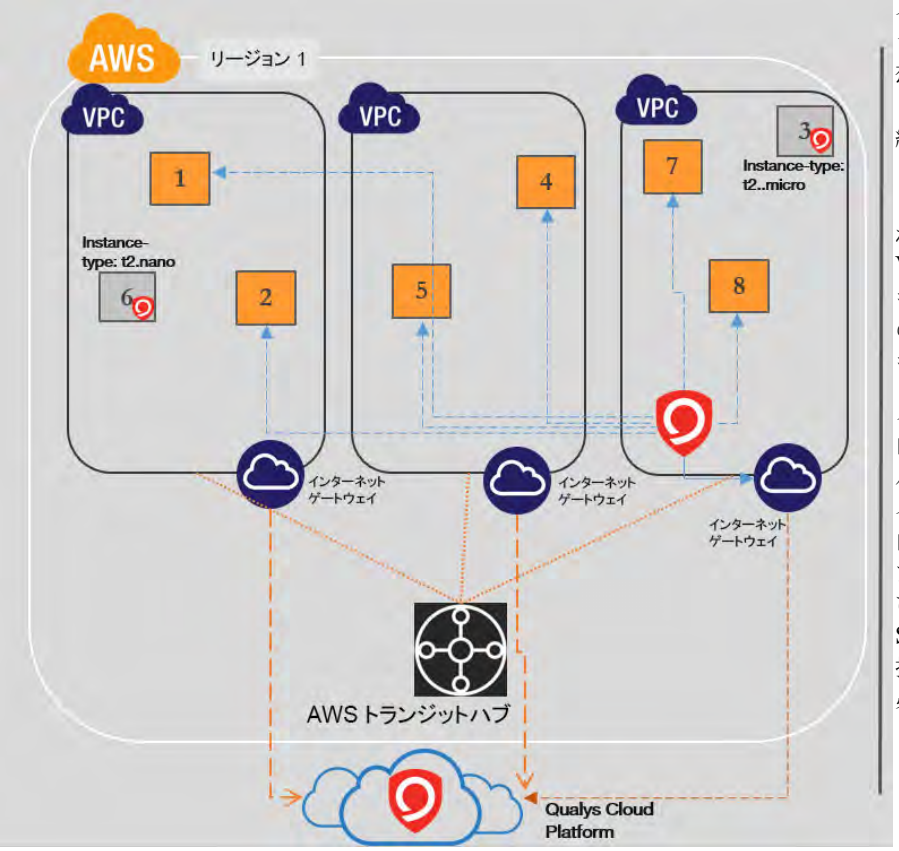


要件に応じてスキャナを追加し、VPC の境界を超えてリージョン間でスキャンができるようにしてください。

スキャナが HTTPS 経由（セキュリティグループおよびインターネットゲートウェイ経由）で Qualys クラウドプラットフォームと AWS EC2 および STS エンドポイントに接続するよう、設定する必要があります。

AWS では、お使いの環境が中断される可能性を最小限にするために、セキュリティ評価から、EC2 インスタンスタイプの T3.nano、T2.nano、T1.micro、M1.small を除外することを推奨しています。これらをスキャンする場合は、Cloud Agent の使用を推奨します。

トランジットによって接続されたリージョン内の VPC 間で 1 つのスキャナが複数のインスタンスをスキャンする場合

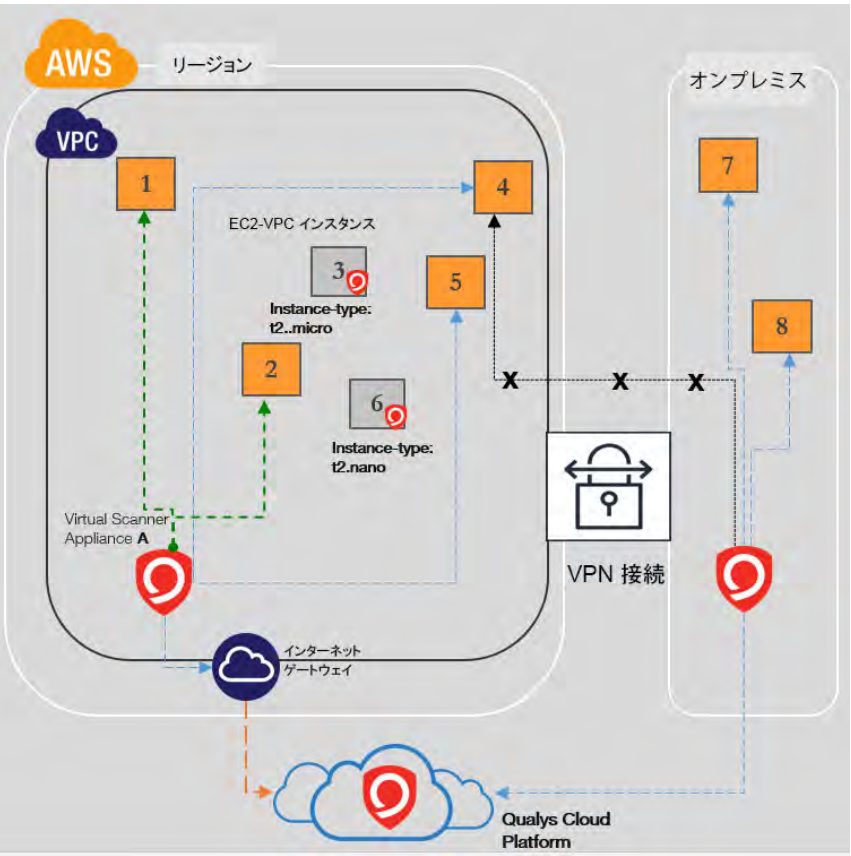


ネットワークトランジットハブにより、仮想プライベートクラウド（VPC）間の相互接続が可能になるため、トランジットゲートウェイによって接続されたリージョン内の VPC 間で 1 つのスキャナを使用して複数のインスタンスをスキャンできます。

スキャナを HTTPS 経由（セキュリティグループおよびインターネットゲートウェイ経由）で Qualys クラウドプラットフォームおよび AWS EC2 および STS エンドポイントに接続するよう設定する必要があります。

AWS では、お使いの環境が中断される可能性を最小限にするために、セキュリティ評価から、EC2 インスタンスタイプの T3.nano、T2.nano、T1.micro、M1.small を除外することを推奨しています。これらをスキャンする場合は、Cloud Agent の使用を推奨します。

クラウドインスタンスのスキャンにオンプレミスのスキャナが推奨されない場合



スキャナが HTTPS 経由（セキュリティグループおよびインターネットゲートウェイ経由）で Qualys クラウドプラットフォームと AWS EC2 および STS エンドポイントに接続するよう、設定する必要があります。

オンプレミスのネットワークにあるスキャナは、クラウド対応ではなく、スキャンのワークフローが従来型であるため、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。

AWS の侵入テストルールに従って、インスタンスタイプの t2.micro と t2.nano はスキャンされません。これらをスキャンする場合は、Cloud Agent の使用を推奨します。

センサの配置

Qualys クラウドプラットフォームの中核的なサービスである Qualys センサを使用すると、グローバルな企業全体に対してセキュリティを容易に拡張することができます。センサは、リモートからの配置と一元管理が可能であり、自己更新機能を備えています。センサにより、データが収集され、Qualys クラウドプラットフォームに自動的に送信されます。Qualys クラウドプラットフォームには、脅威を特定して脆弱性を除去するために、情報の分析と相関付けを継続的に行う計算処理能力が備わっています。AWS の場合、センサは AMI および軽量エージェント形式の仮想アプライアンスです。

スキャンを行う前に、センサを配置する必要があります。設定に応じて、事前認証済みの Scanner Appliance を配置することも、Qualys Cloud Agent を配置することもできます。このようなセンサの配置に関する手順について、詳しく説明していきます。

事前認証済み Virtual Scanner Appliance の配置
Qualys Cloud Agent の配置

事前認証済み Virtual Scanner Appliance の配置

事前認証済みスキャナの配置に関する実際の手順に進む前に、ライセンス / コスト面と、配置の推奨事項について説明します。

コストとライセンス

Qualys Virtual Scanner Appliance は、Amazon Machine Image（AMI）として AWS Marketplace から入手可能で、Amazon EC2-Classic および EC2-VPC での起動に対応しています。

以下の 2 点を考慮する必要があります。

- 仮想スキャナライセンスのサブスクリプションに対する Qualys のコスト

- 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に対する AWS のコスト

Qualys のコスト

実行する Virtual Scanner Appliance の各インスタンスに対して 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 ではなく Qualys から取得されます。そのため、当社の Scanner Appliance は、AWS Marketplace に BYOL（つまり、“ 自分のライセンスを使用する ”）モデルとして掲載されています。Qualys クラウドプラットフォームの UI で定義する Qualys Virtual Scanner Appliance の各プロファイルで、Virtual Scanner Appliance のライセンスを 1 つ使用します。Qualys のサブスクリプションから Virtual Scanner Appliance のプロファイルを削除すると、そのライセンスは解放されて、すぐに再利用できるようになります。

料金の見積りまたは評価の依頼については、Qualys のテクニカルアカウントマネージャまたは Qualys 代理店までお問い合わせください。

AWS のコスト

Virtual Scanner Appliance の各インスタンスは、AWS アカウントの 1 つで開始されます。アプライアンスの実行に対する AWS のコストの支払いは、お客様のご負担になります。

このコストには以下が含まれます。

- インスタンスのタイプに基づいた計算処理能力
- ストレージ
- データの双方向の転送

インスタンスを実行する場合、計算処理能力（CPU や RAM など）にかかる料金が、大部分を占めることになります。Scanner Appliance は常時実行する必要はないことに留意してください。インスタンスが停止している時間に発生するのは、ギガバイト単位で課金されるストレージ料金のみになります。ただし、スキャナはソフトウェアとシグニチャを最新の状態に保つために、週に数時間は実行する必要があります。

スキャナ配置の推奨事項

ネットワークトポロジと Scanner Appliance をホストする EC2 インスタンスのサイズに基づくスキャナの配置についての推奨事項を以下に示します。

スキャナをホストするインスタンスのサイズ

Qualys Virtual Scanner Appliance をホストする場合に Qualys が推奨する最大限は、16 CPU および 16 GB RAM です。また、A1 インスタンスタイプへのスキャナ配置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応じて、最大 16 CPU および 16 GB RAM までスケールアップすることができます。

スキャン対象の制限

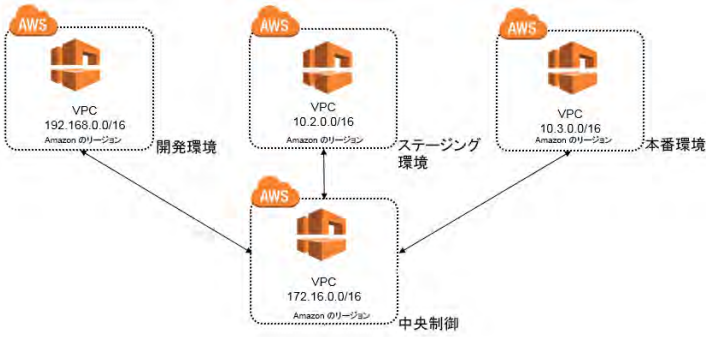
インスタンスタイプ t1.micro、m1.small、t2.nano を使用する対象に対してスキャンは開始できないので注意してください。

ネットワークトポロジに基づいたスキャナ配置

Amazon Virtual Private Cloud（Amazon VPC）は、AWS の顧客に 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提供する包括的な仮想ネットワーク機能を実現しています。Amazon VPC を使用すると、顧客は自分の AWS リソースをホストするために論理的に分離された仮想ネットワークを用意することができます。AWS ネットワークの設定方法に基づいて、スキャナの配置する方法にはいくつかの推奨事項があります。

- リージョン内にピアリング接続されている VPC がない場合 - Qualys では VPC がピアリング接続されていない場合、各リージョンで VPC ごとに 1 つ以上のスキャナを設定することをお勧めします。

- リージョン内にピアリング接続された VPC がある場合 - リージョン内の他の VPC にピアリング接続された中央 VPC に 1 つ以上のスキャナを設定できます（n 個のハブ & スポークモデル）。同様の例を次に示します。



- リージョンを横断する VPC の場合 - VPN のある VPC または他のリージョンへの中継 VPC に 1 つ以上のスキャナを設定できます。

インスタンスのスナップショット / クローニングは不可

新しいインスタンスを作成するために、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ニングを行うことは禁止されています。新しいインスタンスはスキャナとして機能しません。すべての設定内容とプラットフォームの登録情報が失われます。これは、元になったスキャナの障害やエラーにつながる可能性もあります。

インスタンスの移動 / エクスポートはできません

仮想化プラットフォーム（HyperV、VMware、XenServer）で登録済みのスキャナインスタンスを AWS クラウドプラットフォームへ移動またはエクスポートすることは、どのようなファイル形式であっても禁止されています。これによりスキャナの機能が破損し、スキャナのすべての設定が永久に失われます。

必要事項

アカウントで「Virtual Scanner」オプションが有効になっている必要があります。このオプションを有効にするには、Qualys の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。

「Manage virtual scanner appliances」のパーミッションを持つマネージャまたはサブユーザである必要があります。このパーミッションはユニットマネージャに付与することもできます。スキャナにこのパーミッションを付与できるようにサブスクリプションを設定することができます。

スキャナの配置

スキャナの配置には、AWS の設定に加えて Qualys の設定も伴います。

考慮事項

以下の機能はサポートされていないため、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。

- WAN/ 分割ネットワーク設定 - 分割ネットワーク設定のための「WAN Interface」オプションは、スキャナの UI/ コンソールから使用できません。クラウド UI からの LAN/ シングルネットワーク設定のみがサポートされています。これはスキャンと Qualys サーバへの接続の両方に使用されます。

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

- 静的 VLAN（IPV4 および IPV6）- 静的 VLAN を設定するための「VLAN」オプションは、Qualys UI から使用できません。

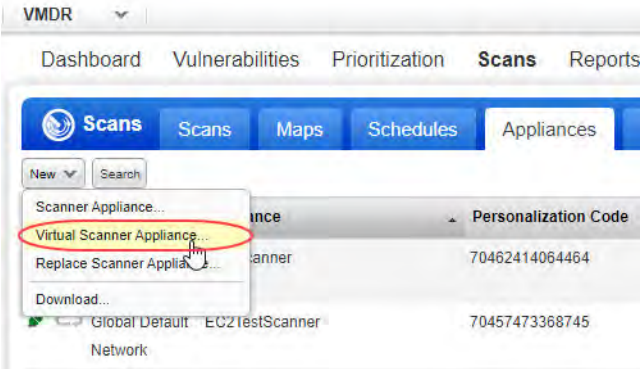
- 静的ルート（IPV4 および IPV6）- “ 静的ルート ” を設定するためのオプションは、Qualys UI から使用できません。

- “ IPv6 on LAN ” - “ IPv6 on LAN ” を設定するためのオプションは、Qualys UI から使用できません。

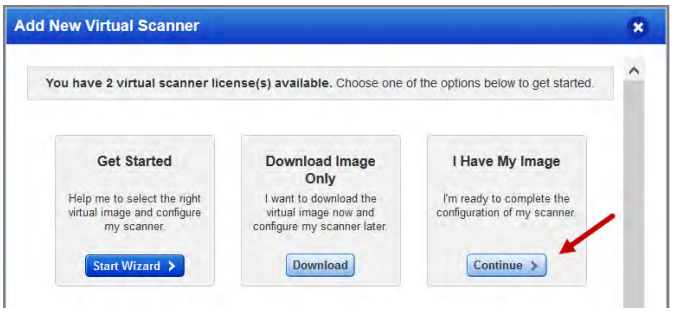
Qualys の設定

Virtual Appliance の設定 - 個人設定コードの取得

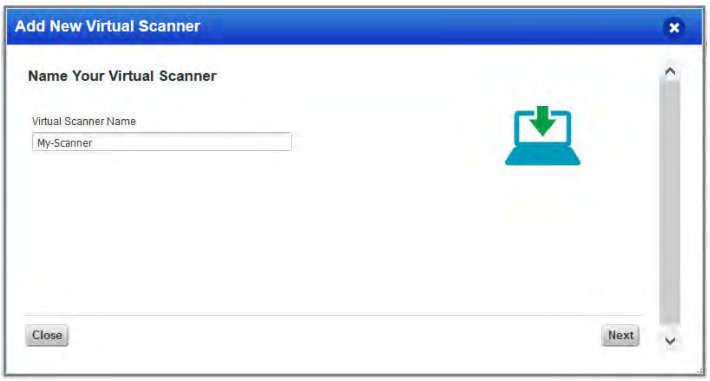
Qualys アプリケーションピッカーから VM/VMDR または PC を選択します。「Scans」→「Appliances」に移動し、「New」→「Virtual Scanner Appliance」を選択します。



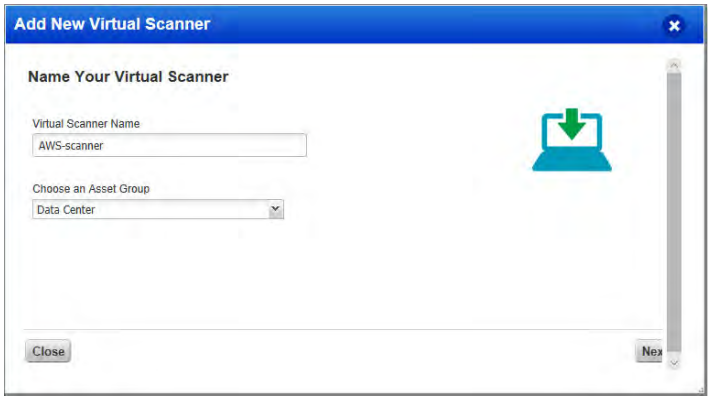
「I have My Image」を選択し、「Continue」をクリックします。



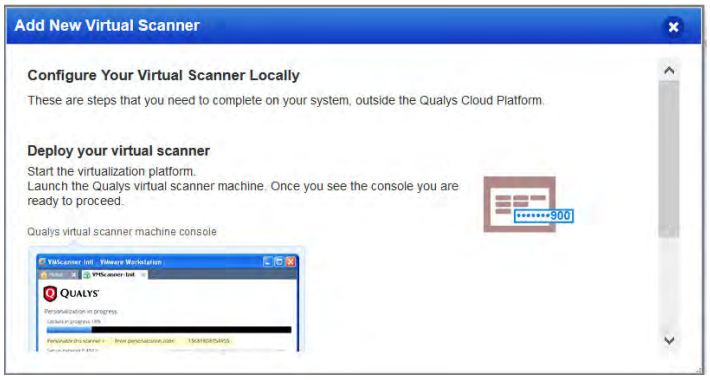
名前を入力して、「Next」をクリックします。



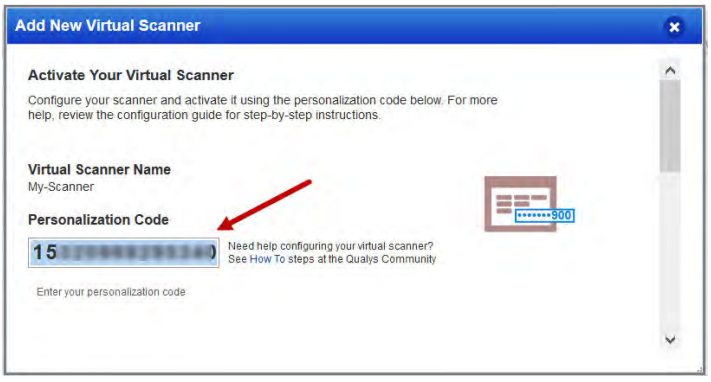
サブユーザの場合は、マネージャユーザがサブユーザのビジネスユニットに割り当てられているアセットグループを選択する必要があります。アセットグループが表示されない場合は、ビジネスユニットのマネージャにアセットグループ（「All」グループ以外の）を割り当てるよう依頼してください。



画面に表示される指示に従って、仮想スキャナを設定します。「Next」をクリックします。



個人設定コードを取得します。このコードは AMI インスタンスを開始するのに必要になります。



AWS の設定

Amazon AWS での AMI インスタンスの開始

このステップでは、Amazon AWS Marketplace から AMI インスタンスを開始する方法について説明します。AWS Management Console を使用して AMI インスタンスを開始することもできます（コンソールにサインイン後、「Services」→「EC2」に移動し、下記に従って AMI の設定を入力します）。

注記： AWS マーケットプレイスで入手できるイメージ、またはダウンロード可能な AWS 固有のイメージを入手するために Qualys が提供する署名付き URL で入手できるイメージのみを使用していることを確認してください。Qualys UI からダウンロードしたイメージを AWS で使用することは推奨していません。

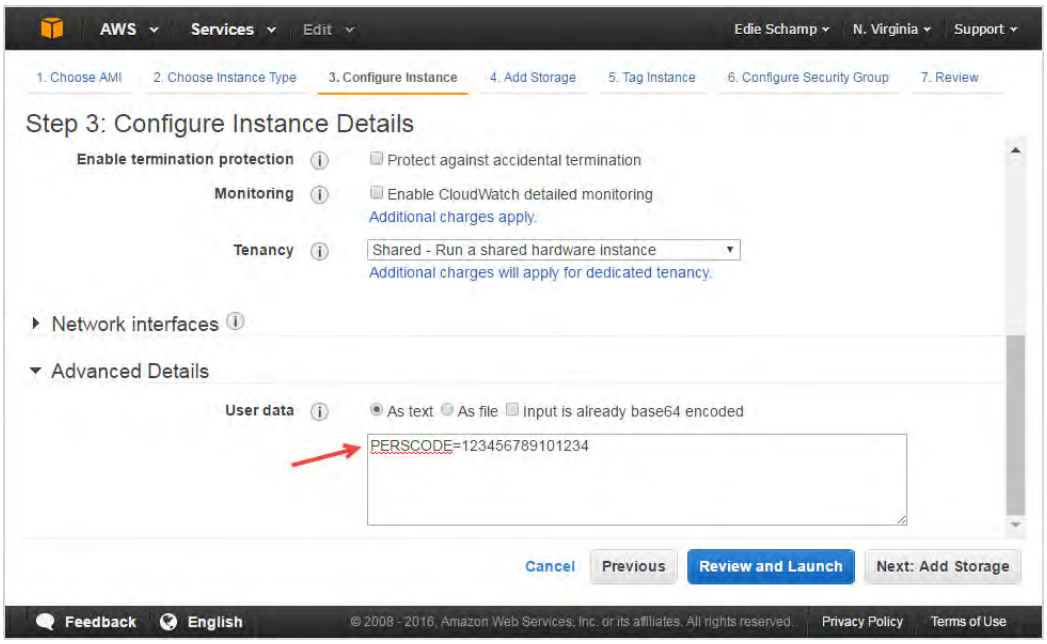
1）AWS Marketplace で Qualys Virtual Scanner Appliance のページに移動し、AWS アカウントにログインします。

AWS Marketplace にある Qualys Virtual Scanner Appliance（事前認証済みスキャン）HVM

AWS Marketplace には、2 つの Virtual Scanner Appliance（事前認証済みの Scanner Appliance と標準の Scanner Appliance）が掲載されています。標準のアプライアンスは、IP ベースのスキャンを実行します。Qualys は、事前認証済みの Scanner Appliance の使用を推奨しています。事前認証済みの Scanner Appliance を使用できない場合は、標準の Scanner Appliance を選択する前に Qualys のサポートにお問い合わせください。

2）リージョンで Virtual Scanner AMI を開始します。

3）ウィザードを使用して、AMI 設定を入力します。「User data」フィールドに Qualys のユーザインタフェースで取得した個人設定コードを入力し、オプションでプロキシサーバを入力します（使用している場合）。



個人設定コード - PERSCODE= に続けて、Qualys で取得した個人設定コードを入力します。

プロキシサーバ（オプション） - PROXY_URL に続けて、個人設定コードとは別の行にプロキシサーバの情報を入力します。プロキシサーバは、スキャナが Qualys クラウドプラットフォームに直接接続されていない場合に使用されます。

プロキシ情報を username:password@proxyhost:port の形式で入力します。
ドメインユーザがある場合の形式は、domain\username:password@proxyhost:port になります。
認証を使用しない場合は、proxyhost:port の形式になります

ここで、proxyhost は IPv4 アドレスまたはプロキシサーバの FQDN、port はプロキシサーバを実行しているポート番号になります。

例：

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

プロキシサーバを使用する場合は、Qualys UI で Amazon EC2 API のプロキシサーバ設定が行われていることを確認します。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。

開始後 Virtual Appliance は Qualys クラウドプラットフォームに接続

このステップでは、Virtual Scanner Appliance が Qualys アカウントに登録されます。また、アプライアンスによって最新のソフトウェア更新がただちにダウンロードされ、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に以下のアウトバウンドルールを設定します。

- Qualys クラウドプラットフォームへの接続性

Scanner Appliance には、Qualys クラウドプラットフォームへの接続性が必要です。Scanner Appliance がインターネットに直接接続している場合は、アウトバウンドルールによってポート 443 で Qualys セキュアオペレーションセンター（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 IP アドレスの範囲は、Qualys ポータルにログイン後、「ヘルプ」→「一般情報」オプションを選択すると取得できます。プロキシサーバを使用している場合は、アウトバウンドルールでプロキシサーバとの通信が許可されており、プロキシサーバが Qualys クラウドプラットフォームと通信できることを確認します。

- Amazon EC2 API エンドポイントへの接続性

Scanner Appliance は、Amazon EC2 および STS API エンドポイントに接続する必要があります。認証を受けるために、スキャナは STS エンドポイントにアクセスして、EC2 API 呼び出しを実行するためのロールとトークンを取得します。EC2 および STS API への接続は、Qualys クラウドプラットフォームとのアプライアンス管理通信用にプロキシサーバを設定している場合でも、プロキシサーバ経由でルーティングされることはありません（上記参照）。Scanner Appliance は、EC2 および STS API に直接接続するか、完全透過プロキシまたはフィルタリングテクノロジを介して接続する必要があります。

Scanner Appliance がインターネットに直接接続している場合は、アウトバウンドルールによってポート 443 で 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 のプロキシサーバを設定している場合は、アウトバウンドルールでプロキシサーバとの通信が許可されており、プロキシサーバが Amazon EC2 API エンドポイントに接続できることを確認します。

Scanner Appliance には、Amazon EC2 API エンドポイントへの接続性が必要です。アプライアンスが Amazon EC2 API エンドポイントに接続できない場合、EC2 をスキャンするために開始したすべてのジョブは失敗します。“ No Hosts alive ” エラーの可能性により、アプライアンスが対象インスタンス ID のリストを IP アドレスに解決することができないため、スキャンは EC2 の対象インスタンスをスキャンすることなく終了します。

リージョンおよびエンドポイントの詳細については、次のサイトを参照してください。
http://docs.aws.amazon.com/general/latest/gr/rande.html#ec2_region

- 対象インスタンスへの接続性

スキャンを実行するには、スキャナがすべての対象インスタンスに接続できる必要があります。スキャナによってスキャンされる 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よう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

EC2 インスタンスのスキャンに Qualys プライベートクラウドプラットフォーム（PCP）を使用している場合は、AWS 用 Virtual Scanner Appliance AMI の生成について Qualys の営業担当（TAM）またはサポートにお問い合わせください。その際、次の情報をご提供ください。

- Scanner Appliance を配置する AWS リージョン

- スキャナの配置に使用する AWS アカウント

セキュリティグループで、Scanner Appliance から Qualys PCP のポート 443 への通信が許可され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 の配置

当社の革新的な Qualys Cloud Agent プラットフォームを使用すると、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する軽量の Cloud Agent を導入することができます。

Cloud Agent の機能

- ポート 443 を使用して Qualys クラウドプラットフォームと通信し、プロキシ設定をサポートします。

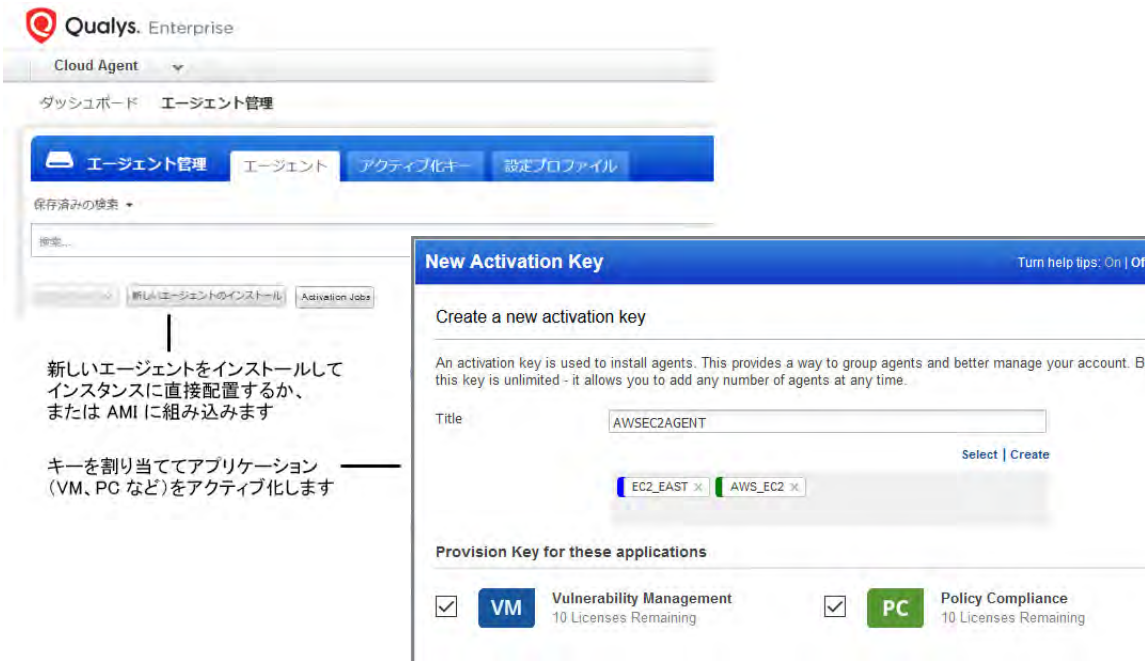
- EC2 インスタンスへの直接配置、または AMI への組み込みを行います。クラウドバーストや揮発性インスタンスも問題なく動作します。

- Linux および Windows OS の各バージョンでのスキャンをサポートします。

- EC2 インスタンスの OS 脆弱性のスキャンをサポートします。

操作手順

Cloud Agent（CA）アプリケーションに移動して、Cloud Agent をインストールします。



推奨リソース

Qualys クラウドプラットフォーム

Qualys Cloud Agent 操作ガイド

アセットのスキャン

ネットワークをスキャンする手順について説明します。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 スキャンのチェックリスト

Qualys VM/VMDR または Qualys PC に移動します。スキャンを始める前に以下の手順を行うことをお勧めします。

- アプライアンスのステータスのチェック

- Qualys UI での Amazon EC2 API プロキシ設定の定義 （プロキシサーバを定義している場合のみ）

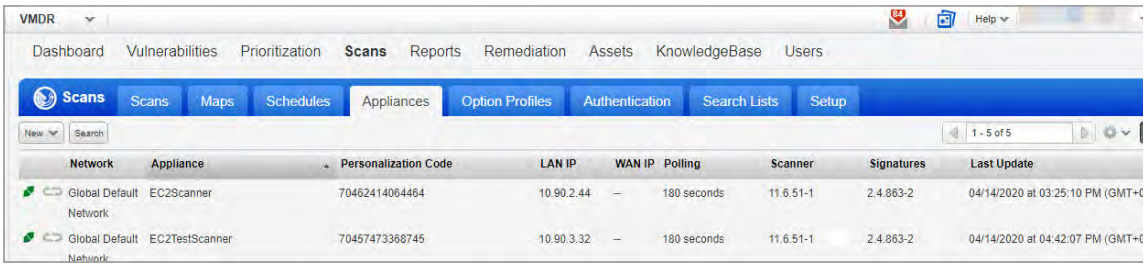
- EC2 アセットがアクティブ化されていることの確認

- スキャンする EC2 インスタンスに対するセキュリティグループの設定

- OS 認証の設定

アプライアンスのステータスのチェック

「Scans」→「Appliances」に移動し、新しい Scanner Appliance が Qualys クラウドプラットフォームに接続されていることを確認します。 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表します。



Qualys UI での Amazon EC2 API プロキシ設定の定義

このステップは、事前認証済みスキャナの配置中に、「User Data」フィールドにプロキシサーバを設定した場合にのみ必要になります。このステップを実行しないと、EC2 スキャンは動作しません。

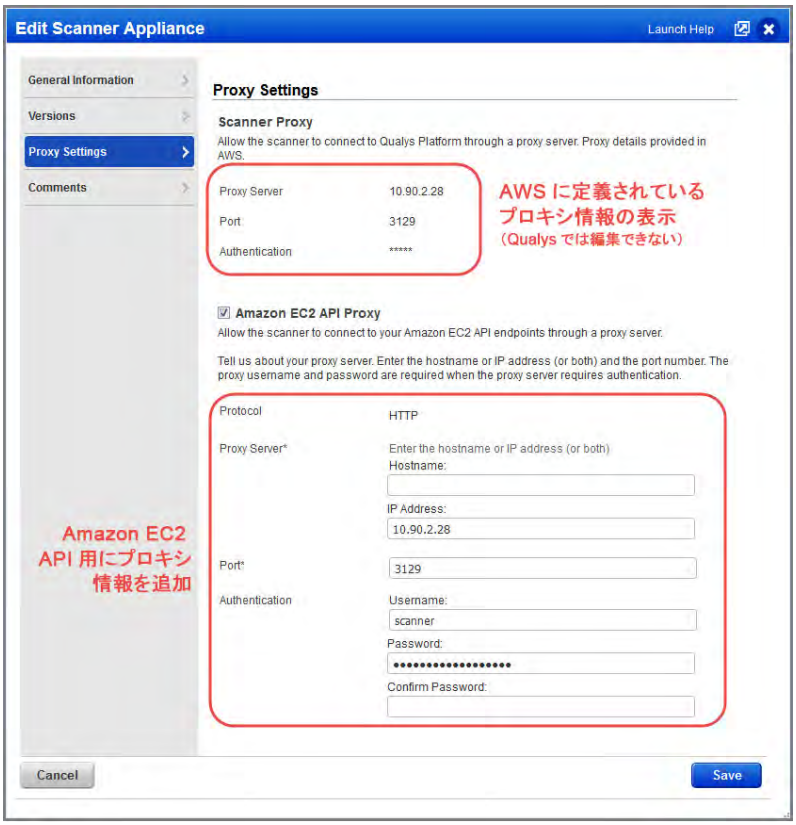
「Scans」→「Appliances」に移動し、EC2 の Virtual Scanner Appliance を編集します。「Proxy Settings」タブに移動し、「Amazon EC2 API Proxy」チェックボックスを選択してプロキシサーバの設定（ホスト名 /IP アドレス、ポート、プロキシの資格情報（プロキシサーバによって求められる場合）など）を入力します。

役立つヒント - ここに入力した設定によって、Virtual Appliance が Amazon EC2 API エンドポイントに接続できるようになります。Virtual Appliance は、指定したプロキシサーバを経由して AWS ゲートウェイへの API 呼び出しを行います。例えば、DescribeInstance API を呼び出して、スキャン対象の各 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 情報ページに表示されます。「Scans」→「Appliances」に移動して、アプライアンスにマウスポインタを合わせ、「Quick Actions」メニューから「Info」を選択します。「Edit」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」項には、AWS AMI 設定に配置中に、現在定義されているプロキシサーバの情報が（資格情報は *** でマスクされて）表示されます。

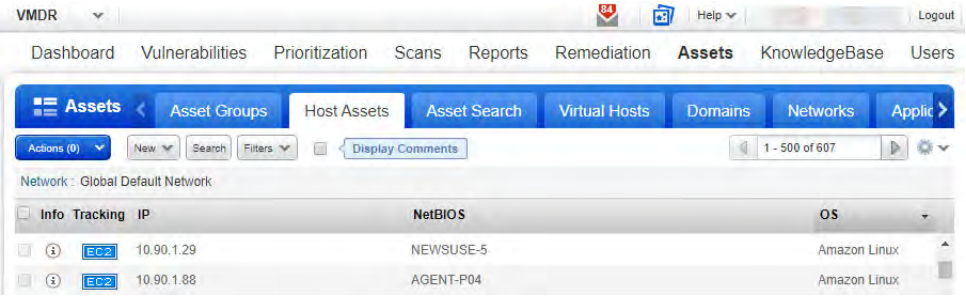


EC2 リージョンのエンドポイントは、プロキシ経由でアクセス可能にする必要があります。

エンドポイントの URL は、http://docs.aws.amazon.com/general/latest/gr/rande.html#ec2_region で確認することができます。

EC2 アセットがアクティブ化されていることの確認

「Assets」→「Host Assets」に移動するか、Qualys AssetView（AV）で、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は、EC2 の追跡方法に割り当てられます。



スキャンする EC2 インスタンスに対するセキュリティグループの設定

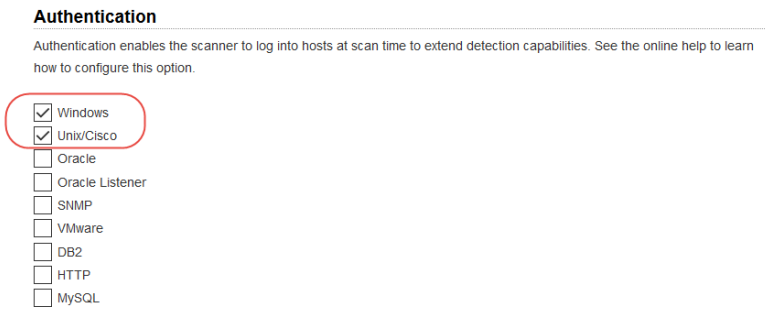
AWS では、Scanner Appliance または Scanner Appliance のセキュリティグループの IP アドレスのすべてのポートに、インバウンドアクセスを許可するセキュリティグループを関連付ける必要があります。

次に示すのは、Qualys Virtual Scanner Appliance のセキュリティグループのすべてのポートに対して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。

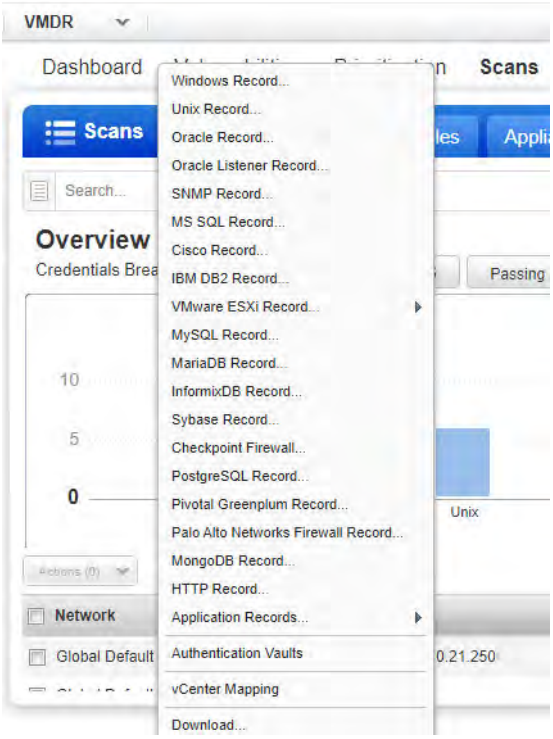
OS 認証の設定

ホスト OS 認証（信頼できるスキャン）を使用すると、スキャン中に各対象システムにログインできます。認証スキャンを実行すると、誤検出を減らし、正確な結果を得ることができます。

「Scans」→「Option Profiles」に移動します。プロファイルの「Initial Options」を編集し、「Save As」を使用してプロファイルを別の名前で保存します。この新しいプロファイルで、必要な認証タイプを有効化します。



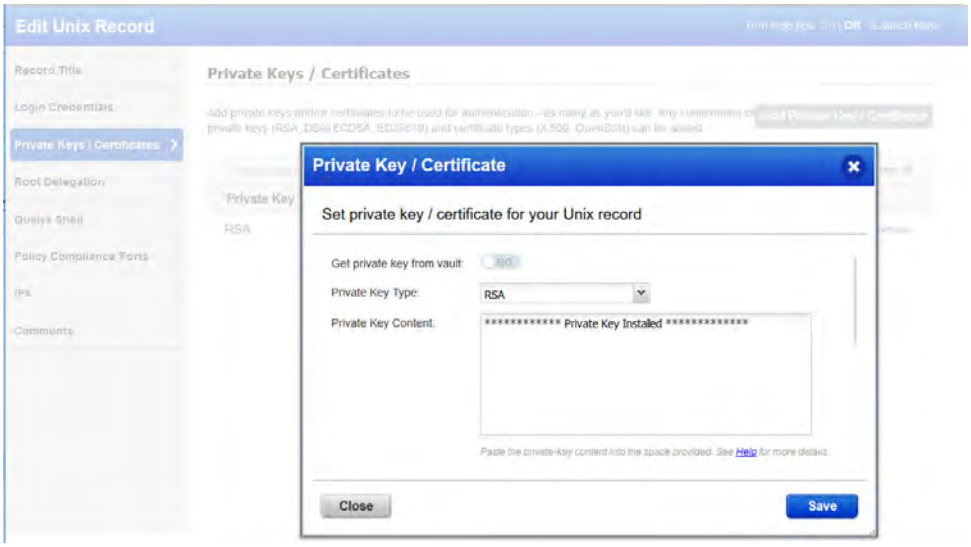
「Scans」→「Authentication」に移動します。スキャンする EC2 インスタンスの認証レコード（Unix や Windows など）を追加します。認証で使用するアカウントの資格情報を認証レコードに追加する必要があります。これは OS ユーザのアカウントであり、AIM ユーザのアカウントではありません。対象のシステムで認証用に専用のアカウントを作成することをお勧めします。



Unix レコードの例

1）ログイン資格情報 - OS のユーザ名を入力し、「Skip Password」オプションを選択します。

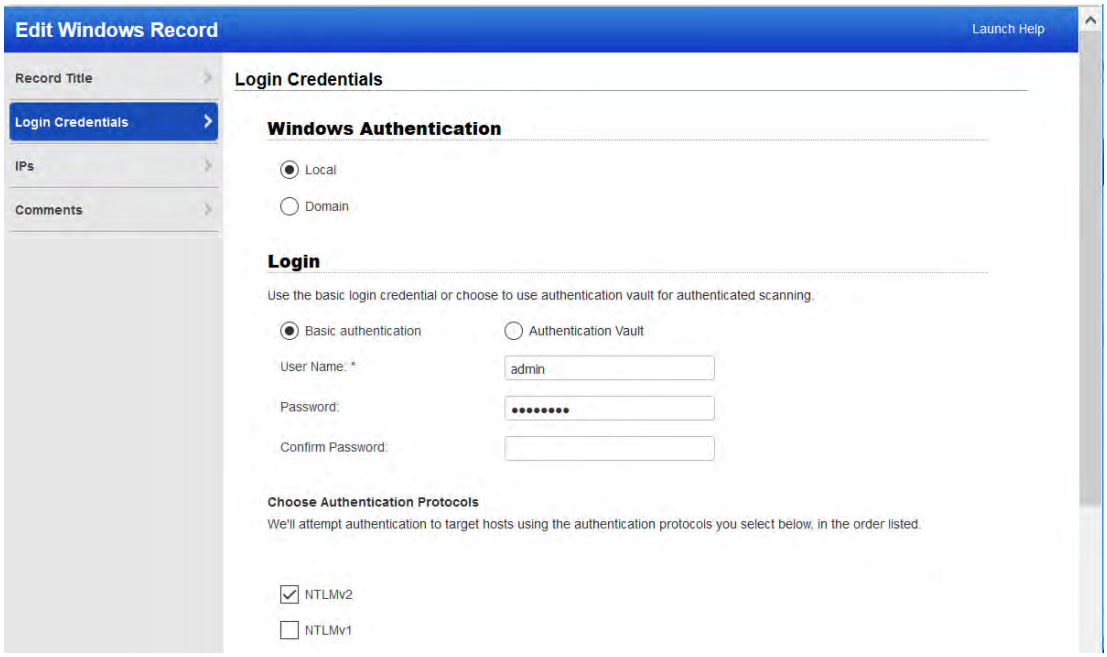
2）秘密鍵 - 鍵認証をお勧めします。鍵のタイプ（RSA、DSA、ECDSA、ED25519）を選択し、秘密鍵のコンテンツを入力します。



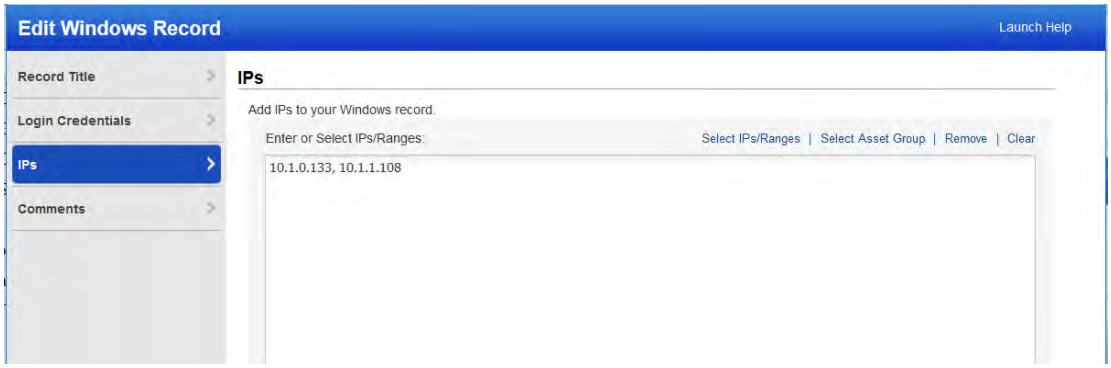
3）IP - この認証レコードの EC2 インスタンスの Unix IP アドレス / 範囲を選択します。このレコードの資格情報は、これらのアセットのスキャンに使用されます。

Windows レコードの例

1）ログイン資格情報 - OS のユーザ名を入力し、「Skip Password」オプションを選択します。



2）IP - この認証レコードの 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に含まれるオンラインヘルプには、詳細な手順と使用可能なすべてのオプションについての説明があります。これらの文書を参照のために使用すると便利です。

Qualys Windows 認証ガイド（PDF、英語）

Qualys Unix 認証ガイド（PDF、英語）

Qualys で定義したネットワークがある場合の Virtual Appliance の移動

このステップは、お客様の Qualys アカウントでカスタムネットワークを定義済みである場合に推奨されます。

デフォルトでは、新規の Virtual Scanner Appliance は、グローバルデフォルトネットワークに配置され、スキャンが実行されると、ホストスキャンデータがこのネットワークに追加されます。スキャンを行う前に、この Virtual Appliance を必要なネットワーク（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）に移動しておくことをお勧めします。

「Assets」→「Networks」に移動し、Virtual Appliance を移動するネットワークを編集して、アプライアンスをこのネットワークに追加します。

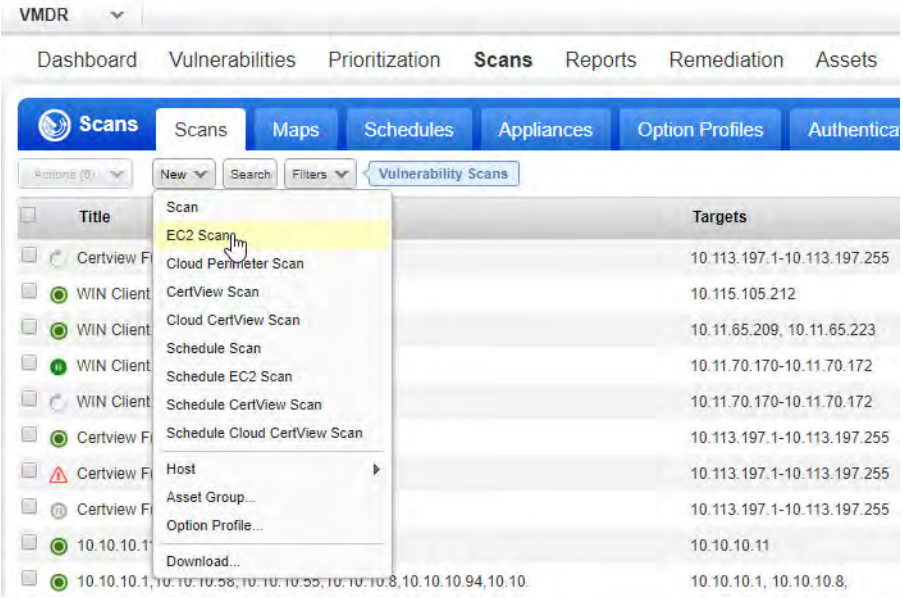
事前認証済み Virtual Scanner Appliance を使用したスキャン

事前認証済み Scanner Appliance を使用したスキャンには、以下のステップがあります。

EC2 スキャンのワークフロー

Qualys には特別な EC2 スキャン（およびスケジュール EC2 スキャン）のワークフローが用意されており、これは事前認証済み Virtual Scanner Appliance で AMI インスタンスをスキャンする場合にのみ動作します。このソリューションにより、顧客は AWS からのスキャンの許可を手動でリクエストする必要がなく、Amazon EC2-Classic および EC2-VPC でのオンデマンドおよびスケジュールによるスキャンが可能になります。

Qualys コミュニティ：AWS のスキャンで受け入れ可能な使用ガイド



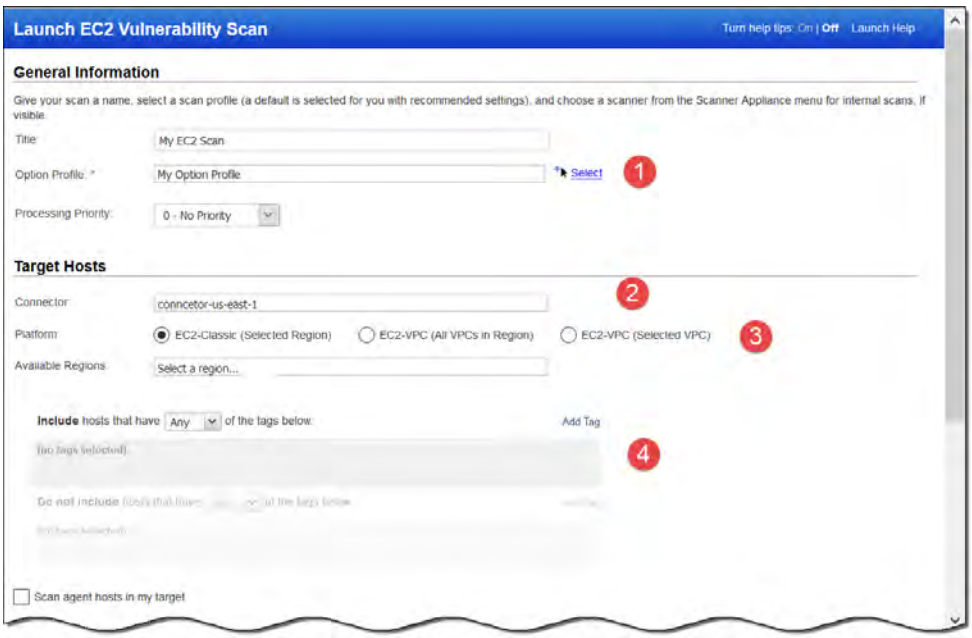
スキャン設定の定義

1）スキャンにタイトルを設定し、認証で設定したオプションプロファイルを選択します（脆弱性スキャンでは必須）。

2）設定した EC2 コネクタ名を選択します。

3）「Platform」の場合、「EC2 Classic」、「EC2 VPC (All VPCs in region)」、または「EC2 VPC (Selected VPC)」から 1 つを選択します。選択に基づいて、リージョンを選択します。

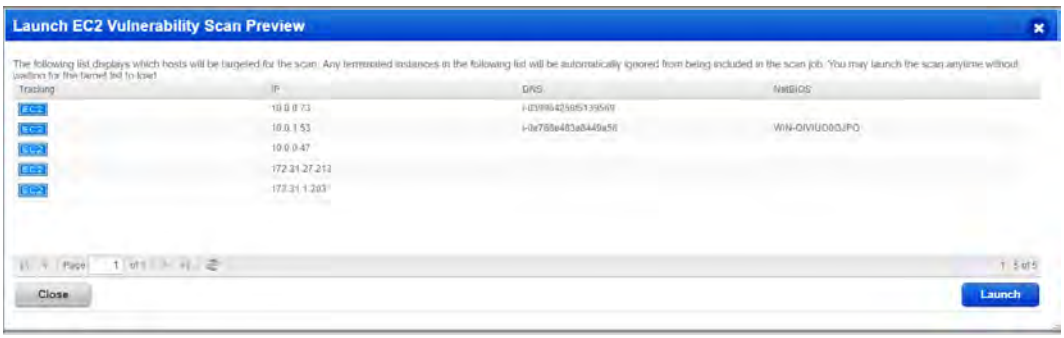
4）アセットタグを選択します。これらはコネクタでアクティブ化されるアセットです。



5）Amazon EC2 で開始した Virtual Scanner Appliance AMI を選択します。

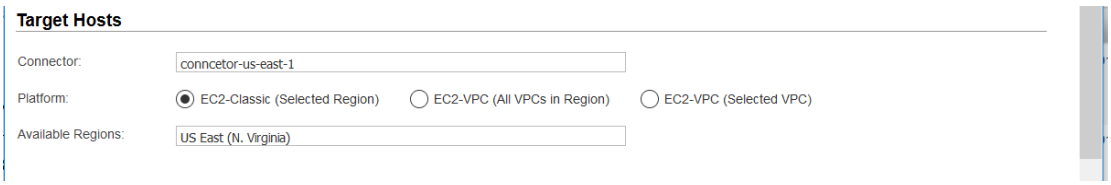
「Launch」をクリックしてスキャンを開始し、Amazon EC2 インフラストラクチャをセキュリティ保護します。

スキャンを開始する前に、「EEC2 Vulnerability Scan Preview」に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、スキャン時にはこのような終了したインスタンスは無視されます。



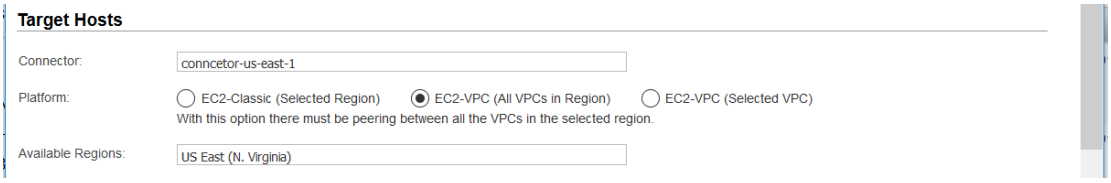
EC2 Classic インスタンスのスキャン

リージョン内の EC2 Classic ホストをスキャンするには、「**EC2 Classic (Selected Region)**」を選択します。このオプションを選択すると、リージョンにある EC2 Classic インスタンスのみがスキャンされます。



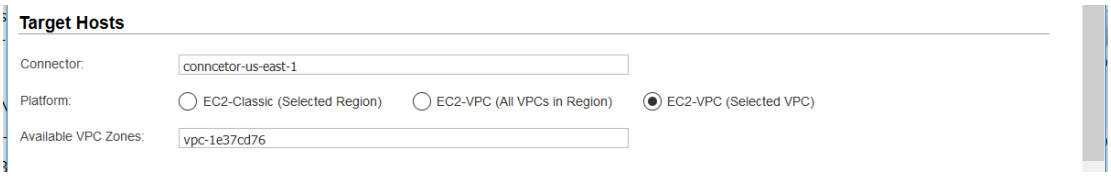
VPC インスタンスのスキャン

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 ピアリング接続を使用したインスタンスのスキャン

リージョン内にあるすべての 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 間でピアリングが確立されている場合にのみ選択します。Virtual Scanner Appliance が VPC にアクセスできないと、インスタンスで「Host not found」エラーが発生する可能性があります。



GovCloud にある EC2 インスタンスのスキャン

Qualys Virtual Scanner Appliance（qVSA）を使用して AWS GovCloud のセキュリティを確保するには、以下の手順に従います。

1）Qualys TAM または Qualys サポートに、a）GovCloud 機能および、b）Qualys Scanner Appliance の事前認証済み AMI へのアクセスを依頼します。

2）スキャナを実行する AWS アカウント ID を追加します。Qualys サポートによって特定のアカウント ID への AMI へのアクセスが有効化されます。

3）Qualys サポートから承認とアクセス情報についての E メールが送信されてきます。

4) “ qVSA ”AMI を使用して Qualys Virtual Scanner インスタンスを作成します。これは、「Create Instance」ウィザードの「MyImages」項で使用できるようになっています（検索を行う必要がある場合は、キーワード “ qVSA ” を使用して Qualys スキャナを検索します）。

5）「スキャナの配置」の説明に従って、Virtual Scanner インスタンスを設定します。

6）これでスキャンを行う準備が整いました。「事前認証済み Virtual Scanner Appliance を使用したスキャン」のステップに従います。

Qualys Cloud Agent を使用した内部ネットワークのスキャン

当社の革新的な Qualys Cloud Agent プラットフォームを使用すると、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する軽量の Cloud Agent を導入することができます。

Cloud Agent の機能

- ポート 443 を使用して Qualys クラウドプラットフォームと通信し、プロキシ設定をサポートします。

- EC2 インスタンスへの直接配置、または AMI への組み込みを行います。クラウドバーストや揮発性インスタンスも問題なく動作します。

- Linux および Windows OS の各バージョンでのスキャンをサポートします。

- EC2 インスタンスの OS 脆弱性のスキャンをサポートします。

はじめに

Cloud Agent（CA）アプリケーションに移動して、Cloud Agent をインストールします。

推奨リソース

Qualys クラウドプラットフォーム
Qualys Cloud Agent 操作ガイド

Qualys スキャナを使用したペリミタースキャン

Qualys スキャナ（インターネットリモートスキャナ）は Qualys クラウドプラットフォームに配置されており、EC2 インスタンスのペリミタースキャンに使用することができます。

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では、内部スキャナの使用が許可されるようにアカウントが設定されることがあります。

これらは、対象の 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、パブリック DNS でスキャンが開始されます。

要件

クラウドペリミタースキャンは、アカウントで以下の機能が有効になっている場合に使用できます。

1）EC2 スキャン、および 2）Scan by Hostname

アカウントには、アカウントに割り当てられている以下のパーミッションが付与されたマネージャまたはユニットマネージャのロールがあることが必要です。

- Enable Cloud Perimeter Scans（外部スキャナを使用したスキャンの開始）

- Enable Internal Scanners for Cloud Perimeter Scans（内部スキャナを使用したスキャンの開始）

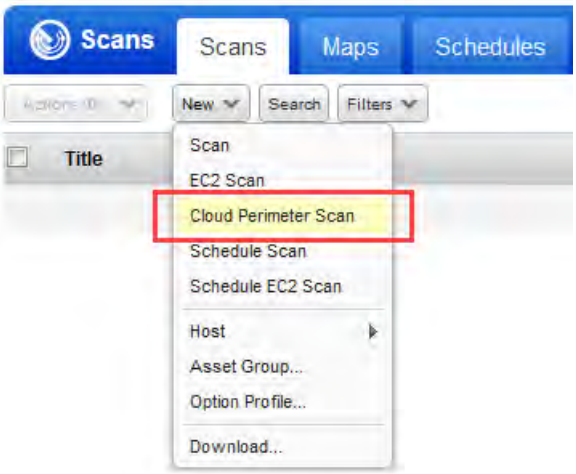
EC2 コネクタが必要です。コネクタからパブリックロードバランサをスキャンに含めるには、CloudView アカウントで同じ EC2 コネクタを設定します。同じ設定のコネクタを作成するには、アカウントに CloudView サブスクリプション、プラットフォームに CloudView のベース URL“ qweb_cloud_view_base_url ” へのアクセス権が必要です。CloudView オンラインヘルプの「AWS コネクタの設定」を参照してください。

スキャンに micro、nano、small インスタンスタイプを含める場合、アカウントでこれらのインスタンスタイプをアクティブ化する必要があります。

操作手順

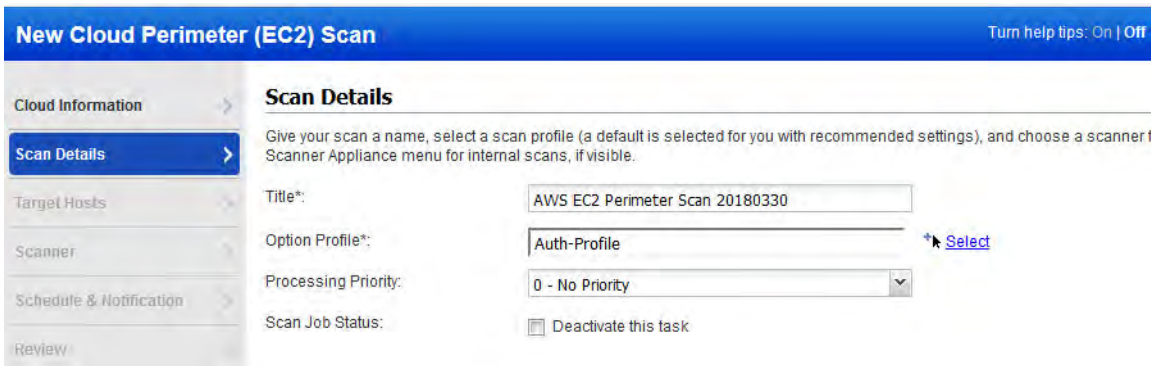
すべてのクラウドペリミタースキャンは、「now」（1 回のみのスキャンジョブ）、または「recurring」のどちらかでスケジュールされます。保存したスキャンジョブは、「Schedules」リストに表示されます。スキャンジョブが開始されると、「Scans」リストに表示されます。

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、「New」→「Cloud Perimeter Scan」を選択します。このオプションは、「Schedules」タブからも選択できます。



最初に行うことは、設定した EC2 コネクタを選択することです。

スキャンにタイトルを設定し、認証で設定したオプションプロファイルを選択します。未認証、または認証済みのクラウドペリミタースキャンのどちらかを開始することができます。



次に、スキャンの対象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の DNS 名を指定しない場合、コネクタから解決されたアセットでスキャンが開始されます。

1）（オプション）プラットフォームオプションを「EC2 Classic」、「EC2 VPC (All VPCs in region)」、または「EC2 VPC (Selected VPC)」から選択します。選択に基づいて、リージョンを選択します。

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ためのオプションもあります。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ついて認証なしのライトポートスキャンの実行を推奨する警告メッセージが表示されます。スキャンに micro、nano、small インスタンスタイプを含める場合は、アカウントでこれらのインスタンスタイプをアクティブ化する必要があることに留意してください。

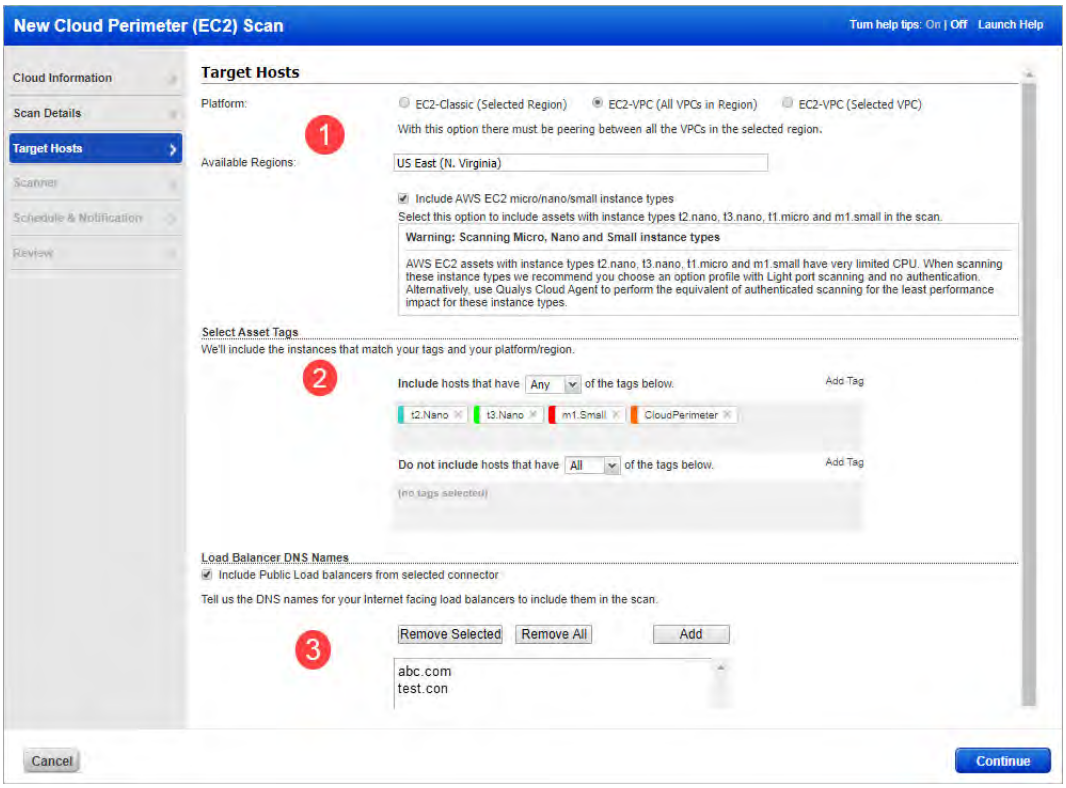
2）（オプション）アセットタグを選択します。これらはコネクタに対してアクティブ化されたアセットです。

3）（オプション）パブリックロードバランサのチェックボックスをオンにして、選択したコネクタから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をサポートしていません。

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ためのオプションもあります。「Add」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設定を持つ CloudView の AWS コネクタからパブリックロードバランサが取得されます。このオプションを選択する場合、CloudView アカウントで、選択したコネクタと同様の設定を持つコネクタを用意しておいてください。CloudView で同じ設定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は取得されません。CloudView 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。

アセットおよびロードバランサを解決する場合に、オプションで選択される “ プラットフォーム ” および “ アセットタグ ” についてコネクタから解決されるアセットまたはパブリックロードバランサがない場合、スキャンはロードバランサの DNS 名で開始されます。ロードバランサの 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。

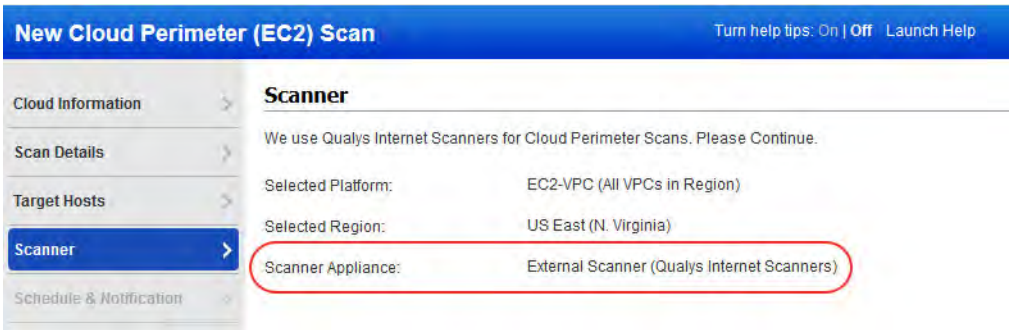


DNS ベースのスキャン

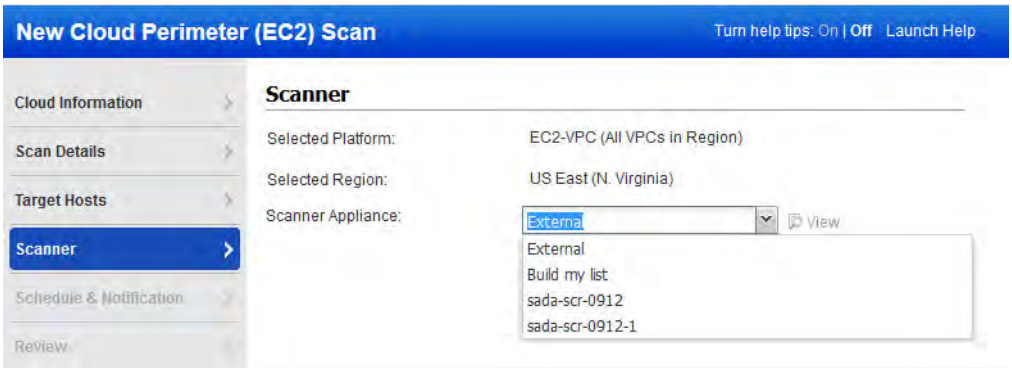
この機能は、使用しているサブスクリプションで有効にする必要があります。この機能を有効にする場合は、Qualys サポートにお問合せください。

DNS ベースのスキャンの動作 : ユーザが ELB などのスキャンを DNS に送信します。IP はリアルタイムで解決されてスキャンされます。

クラウドペリミタースキャンではデフォルトで Qualys 外部スキャナが使用されます。



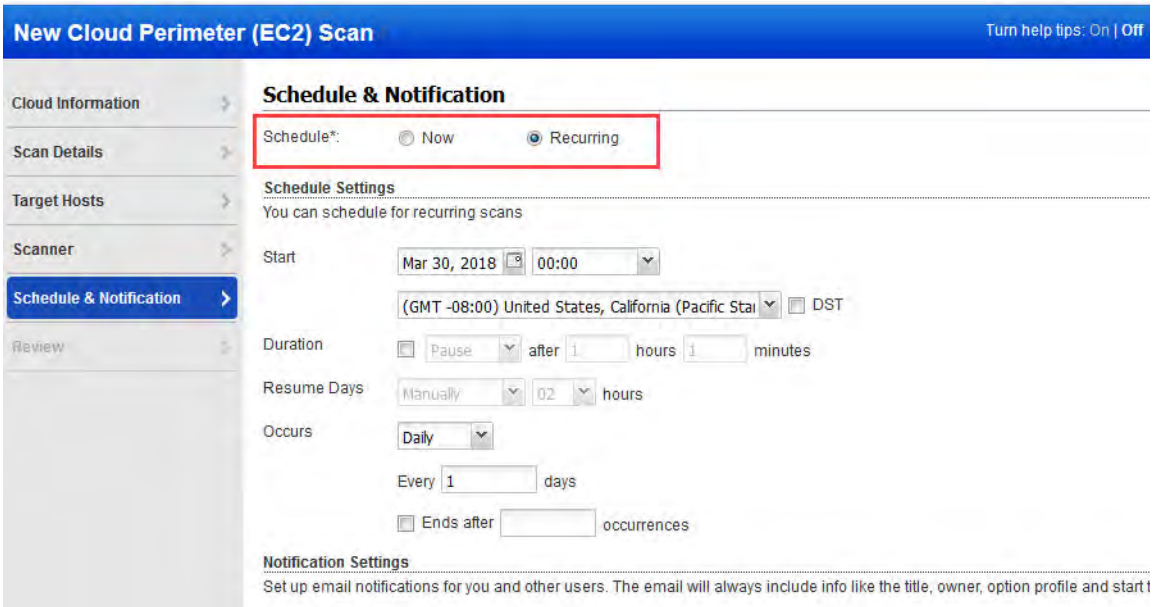
プライベートクラウドプラットフォームの場合、Scanner Appliance がクラウドペリミタースキャンジョブで使用できるようにサブスクリプションが設定されていることがあります。この場合は、リストから 1 つ以上の Scanner Appliance を選択します（「Build my list」オプションを使用）。



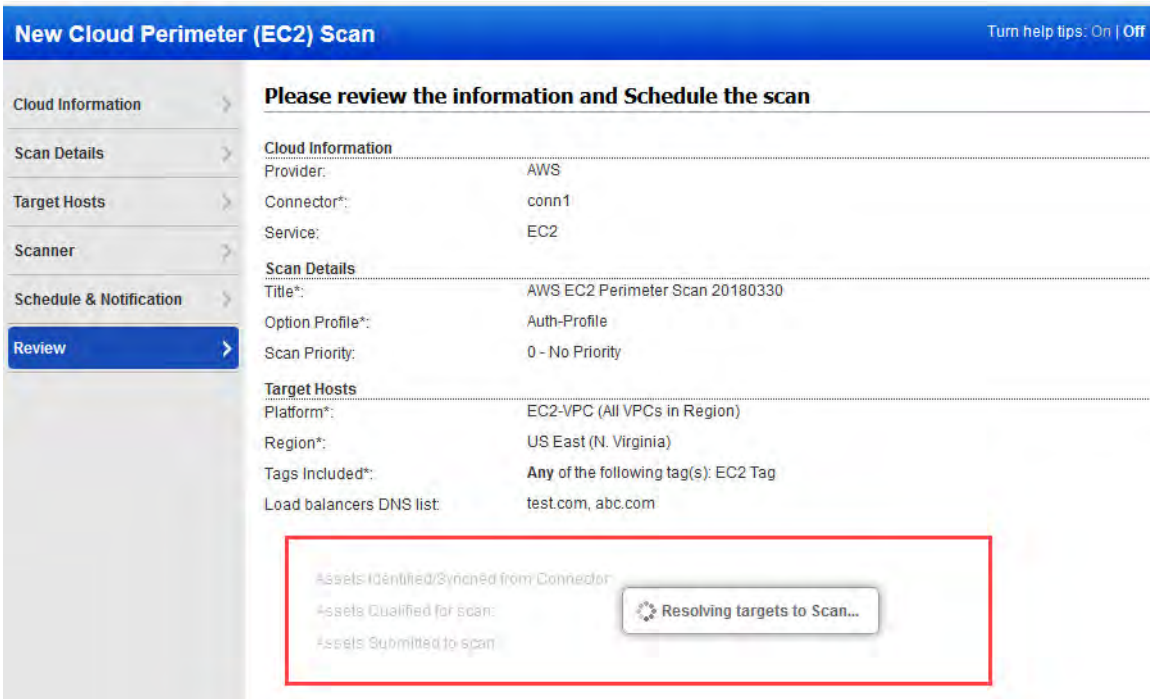
スキャンを実行するタイミングを、「Now」と「Recurring」から選択します。

「Now」を選択しても、スキャンがすぐには開始されないことがあります。新規スキャンリクエストは、数分ごとにチェックされます。スキャナが使用可能であり、同時実行できるスキャンの上限数に達していない場合、スキャンが開始されます。スキャナが使用可能でない、または上限に達している場合、スキャンは次に条件が整ったときに開始されます。

「Recurring」を選択した場合は、スケジュールと通知のオプションも設定します。これらの設定は、他のスキャンスケジュールの設定と同じであるため、使い慣れているはずです。



この設定に基づいて、スキャンするアセットが識別されます。



スキャン対象となるアセット数が表示されます。

「Assets Identified / Synced ト」- このスキャンジョブで選択したコネクタによって検出されたアセットの数です。

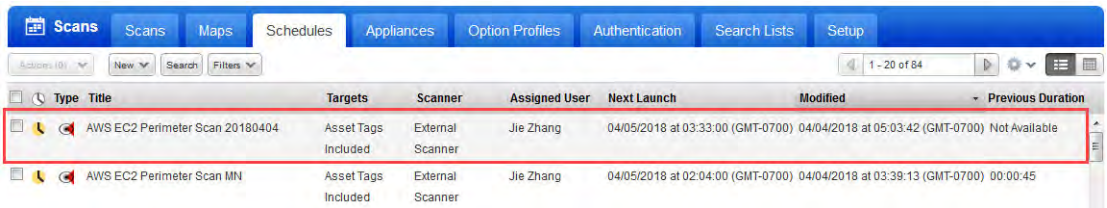
「Assets Qualified for scan」- コネクタによって検出されたアセットのうち、選択されたプラットフォーム、リージョン、アセットタグが一致するアセットの数です。終了したインスタンスは除外されます。

「Assets Submitted to scan」- スキャンジョブで送信されるアセットの数です。条件を満たすアセット（上記のカウント）から、VM で（脆弱性スキャン用に）アクティブ化されていないアセットと、PC で（コンプライアンススキャン用に）アクティブ化されていないアセットを除外したものになります。

準備が整ったら、「Submit Scan Job」をクリックします。

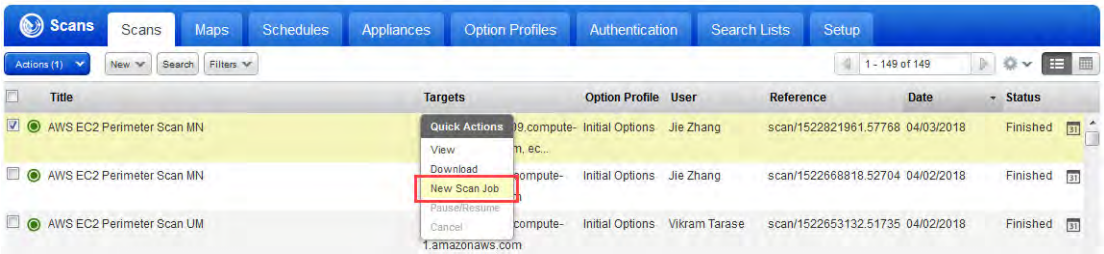
次に実行されること

新しいスキャンジョブは、「Schedules」リストに表示されます。



スキャンが開始されると、「Scans」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、スキャンステータスの表示、結果のダウンロードなどのアクションを実行することができます。

スキャンを再度実行するには、「Quick Actions」メニューから、「New Scan Job」を選択します。特定のスキャン設定を元のスキャンジョブと同じに保ちながら、スキャンスケジュールを「Now」で実行します。



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とファイアウォールのソリューションを使用してアプリケーションのセキュリティを確保することができます。

Qualys WAS

Qualys Web Application Scanning（WAS）には、クロスサイトスクリプティング（XSS）や SQL インジェクションを含むアプリケーションと REST API の脆弱性を識別するために、カスタム Web アプリケーションに対する自動巡回とテストの機能があります。この機能を使用するには、AWS によって事前認証済みの Qualys Virtual Scanner Appliance をインストールします。このアプライアンスは、脆弱性やコンプライアンスを確認するスキャンで使用されるアプライアンスと同じものです。

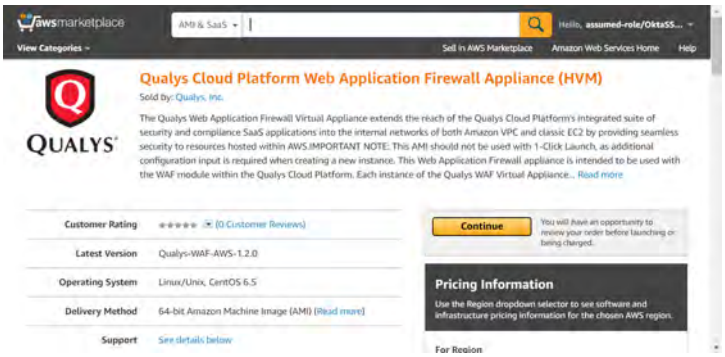
操作手順
- 「スキャナの配置」のステップに従ってください。
- 『Qualys Web Application Scanning 操作ガイド』の手順を参照してください。

Qualys WAF

Qualys Web Application Firewall（WAF）を使用して、ファイアウォールルールと即座に適用される仮想パッチを使用してアプリケーションを保護します。

操作手順
- AWS Marketplace から入手できる Web Application Firewall Appliance をインストールします。
- 『Qualys Web Application Firewall 操作ガイド』の手順を参照してください。

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



分析、レポート、改善

この項では、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作成する方法、AWS ホストの脆弱性管理で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

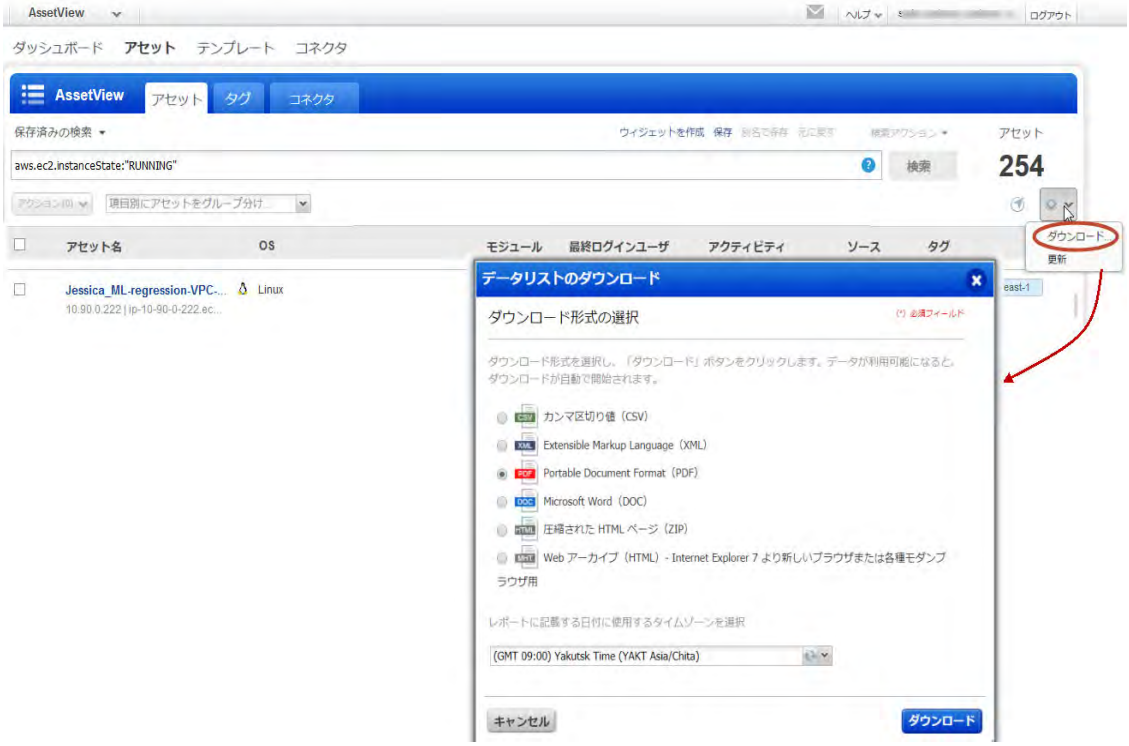
検索機能を使用すると、アセットに関するすべての情報を　1 か所からすばやく検索することができます。AssetView アプリケーションの「アセット」タブに移動します。AWS と入力すると、アカウント ID、インスタンスタイプ、ホスト名など、検索可能なアセットプロパティが表示されます。目的のアセットプロパティを選択します。

クエリの保存

検索内容は、再使用や他のユーザとの共有の目的で、簡単に保存することができます。

検索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は 1 分ほどで終了します。「ツール」メニューから「ダウンロード」を選択します。次に、エクスポートの形式を選択して、「ダウンロード」をクリックします。複数の形式で結果をエクスポートできます（CSV、XML、PDF、DOC、HTML など）。



ウィジェットの作成

アセットで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。例えば、実行中の状態で 1 か月 スキャンされていない AWS アセットを検索します。クエリを入力して「ウィジェットを作成」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に対して、EC2 メタデータ属性を使用して動的タグを作成します。次に動的タグを EC2 スキャン範囲として使用します。「AssetView」→「アセット」→「タグ」を選択し、クラウドアセット検索（AWS EC2 インスタンス）の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

レポートを作成し、EC2 アセットの脆弱性を特定することができます。「レポート」→「レポート」→「新規」→「スキャンレポート」を選択します。次に、事前設定済み、またはカスタマイズされたテンプレートを選択します。

レポートタイトルを設定し、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、イメージ ID や VPV ID などの EC2 インスタンス情報、インスタンスの状態やタイプなどを含めることができます。このインスタンス情報は、ホストの脆弱性の改善と修正のために使用できます。

EC2 アセットのレポートの例を次に示します。

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

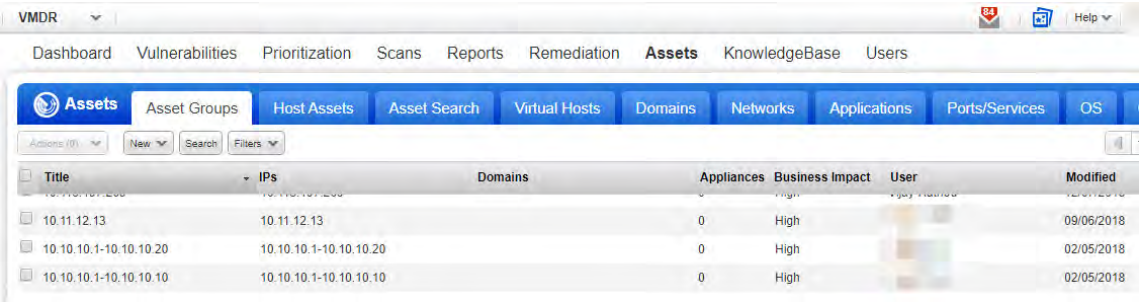
by Status			
Status	Confirmed	Potential	Total
New	0	-	0
Active	10	-	10
Re-Opened	0	-	0
Total	10	-	10
Fixed	0	-	0
Changed	0	-	0

Qualys を使用したアセット管理

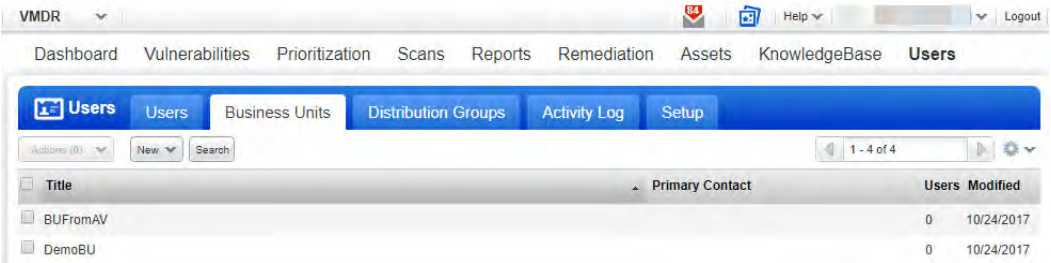
ここでは、Qualys を使用して AWS EC2 インフラストラクチャをセキュリティ保護するためにアセットを編成するためのベストプラクティスとヒントについて説明します。

Qualys の設定

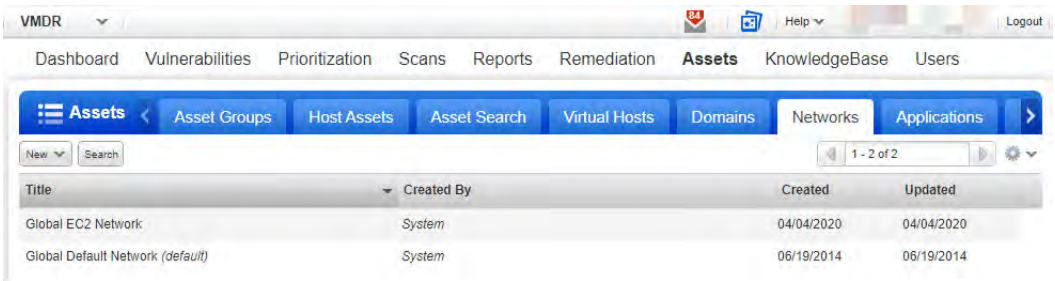
アセットグループ - アセットを意味のあるグループに編成し、サブユーザに割り当てます。アセットグループは、スキャナ、リーダ、ユニットマネージャ（ビジネスユニットが定義されている場合）など、複数のユーザがある場合は必須です。同じ IP アドレスに複数のアセットグループを含めることができます。



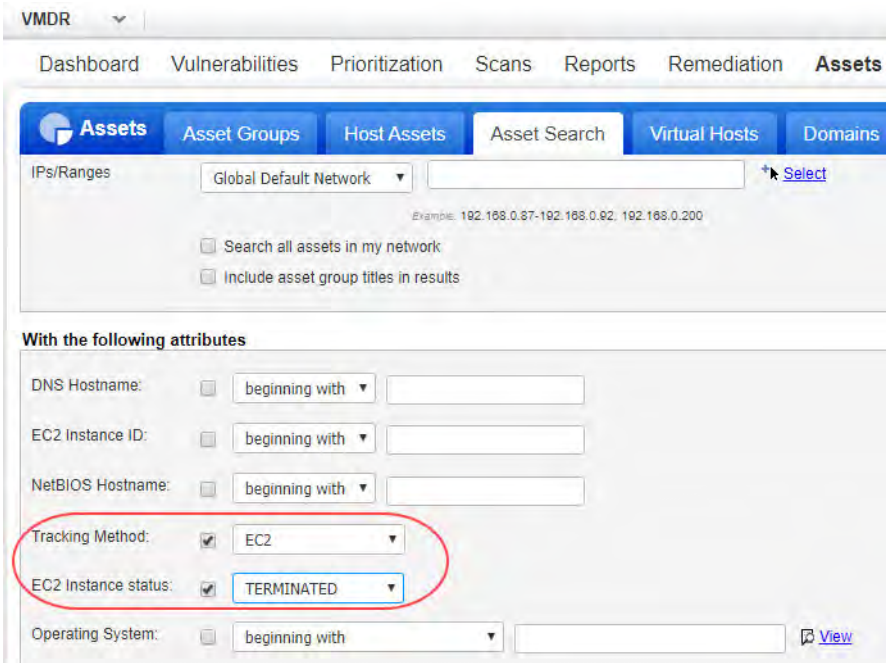
ビジネスユニット - 組織の状態と一致するようにユーザとアセットをビジネスユニットに編成します。こうすることにより、マネージャには、自分に割り当てられたビジネスユニットのコンテキストに沿ってユーザにロールベースのパーミッションを付与できるようになります。同じ IP アドレスに複数のビジネスユニットを含めることができます。



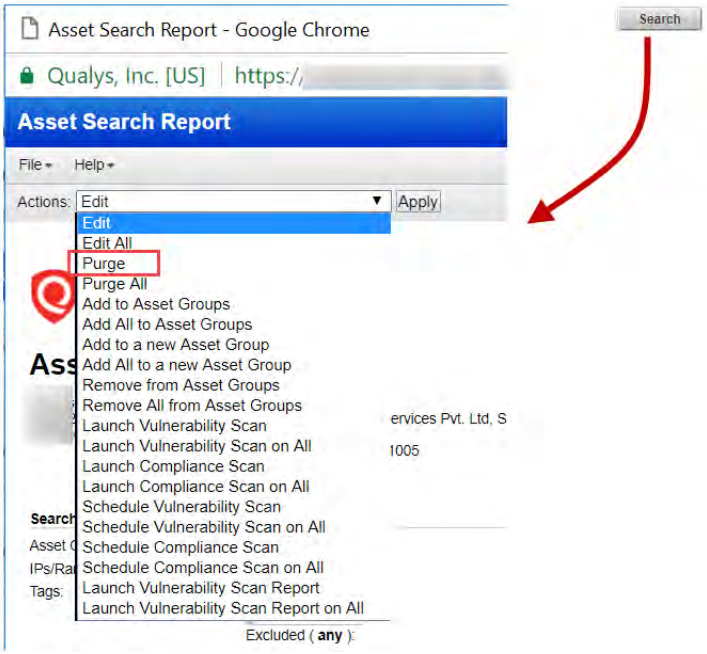
ネットワーク - 重複している IP ブロックを個別に維持するために、独立したプライベート IP ネットワークを編成します。これが設定されると、Qualys はネットワークと IP アドレスを使用して IP を追跡します。IP アドレスは、サブスクリプションまたは 1 つのネットワークに対して一意である必要がある点に注意してください。



終了したインスタンスの削除 - 終了したインスタンスは Qualys アカウントから削除することができます。Vulnerability Management または Policy Compliance で「Hosts」→「Asset Search」に移動して、追跡方法が EC2 であるアセットを選択します。x 日以内にスキャンされていない前回スキャン日などのパラメータを追加して、検索結果を絞り込むこともできます。



「Search」をクリックして、「Actions」メニューから「Purge」を選択します。これにより、アセットとアセットに関連するデータがモジュールから削除されます。



EC2 アセットに Cloud Agent を配置しており、過去 N 日間に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というようなシナリオでは、次の API 呼び出しを使用することができます。

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/"
```

uninstall_agents_not_checkedin.xml のコンテンツ：

```
<?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 ユーザガイド』を参照してください。

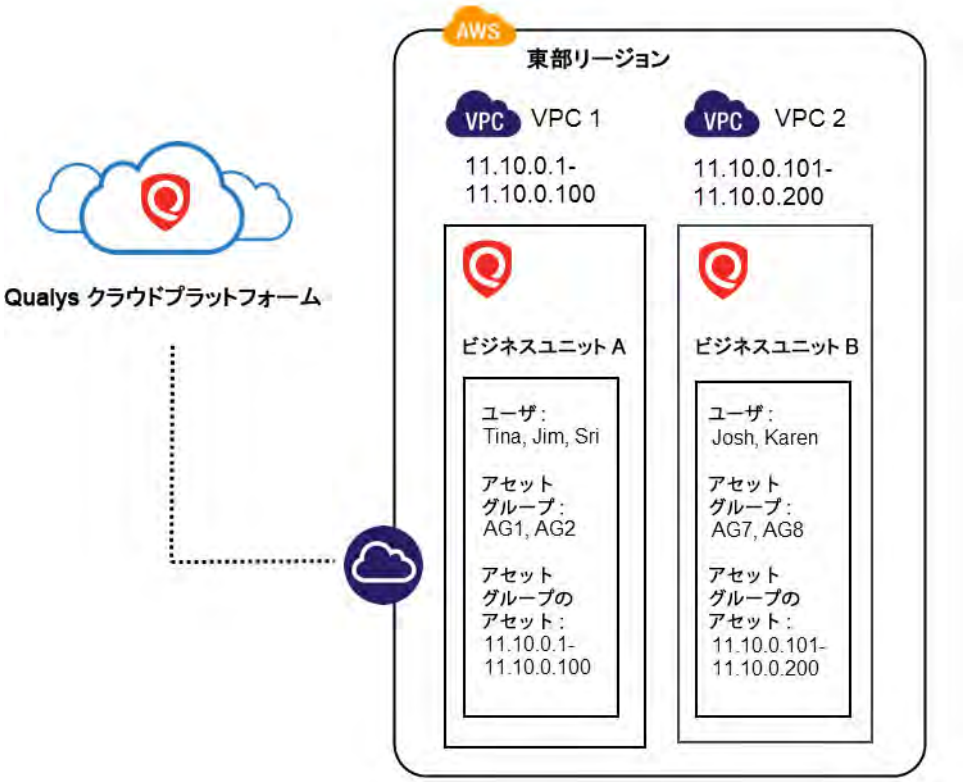
AWS 環境スキャンの使用例

使用例 1 - IP の重複のない複数 VPC のスキャン

- アセットグループの定義は必須ですが、ビジネスユニットはオプションです。

- ビジネスユニットが定義されていると、ユーザのアセットに対するアクセスは自分のビジネスユニット内にあるアセットのみに制限されます。ビジネスユニット A のユーザは、ビジネスユニット B のアセットにアクセスできません。

- アセットグループ AG1、AG2、AG7、AG8 において IP アドレスの重複がない場合のソリューションです。



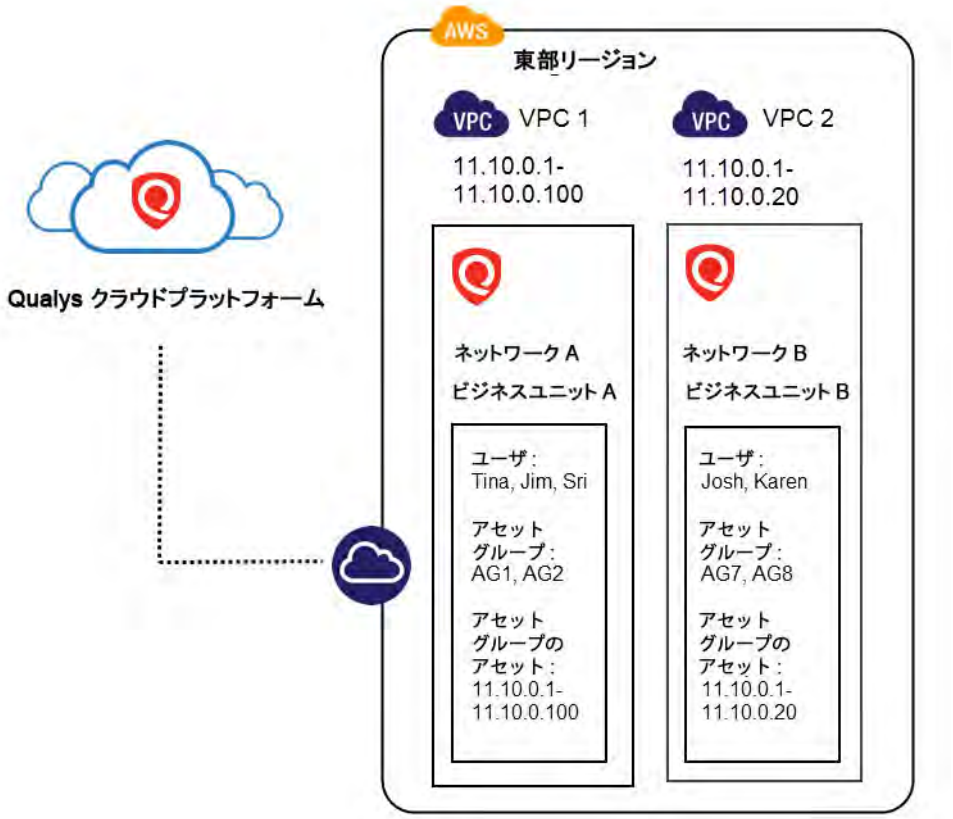
使用例 2 - IP の重複のある複数 VPC のスキャン

- 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ります。

- ビジネスユニットにより、ユーザのアセットに対するアクセスは自分のビジネスユニット内にあるアセットのみに制限されます。ビジネスユニット A のユーザは、ビジネスユニット 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）で IP アドレスの重複がある場合のソリューションです。

注記 : 同じビジネスユニット内に複数のネットワークを設定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強固にできるさまざまな方法を紹介します。

スキャン自動化を DevOps プロセスに統合して AMI を堅牢化

Jenkins からホストおよび EC2 クラウドインスタンスの VM スキャンを自動化

Golden AMI Pipeline

スキャン自動化を DevOps プロセスに統合して AMI を堅牢化

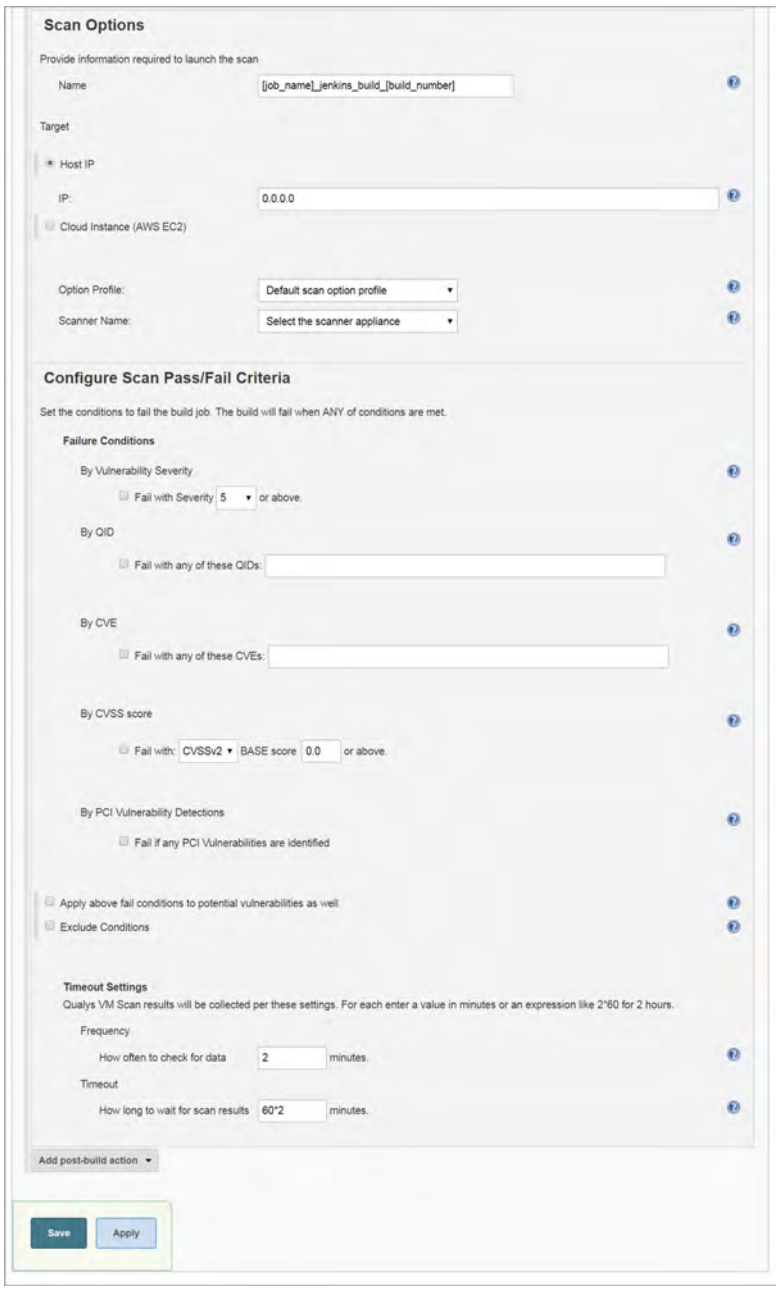
AWS では、公開されている AMI（Amazon Machine Image）を使用して独自のカスタム AMI を作成するのがベストプラクティスです。これにより、事前設定されている OS とソフトウェア上でアプリケーションを実行できるようカスタマイズすることができます。ただし、このようなカスタム AMI は、本番環境のワークロードで使用する前に、包括的なテストを行う必要があります。また、AMI に対して脆弱性スキャンを実行して、アプリケーションの脆弱性やベストプラクティスからの偏差を評価する必要もあります。Qualys では、AMI イメージをスキャンするために、DevOps プロセスに統合するためのすぐに使用できる API を提供しています。

例えば、下の図には、AMI の作成と、AMI を堅牢にするために Qualys API を使用する方法についての一般的なステップが示されています。

AWS に関連する Qualys API の使用の詳細については、『アセット管理およびタグ付け API v2 ユーザガイド』（PDF、英語）を参照してください。

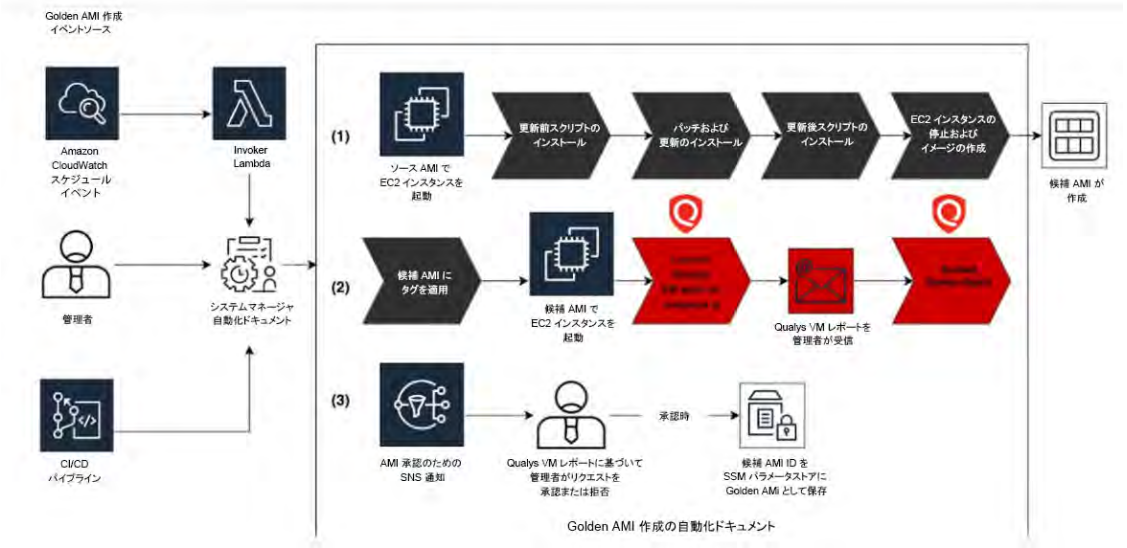
Jenkins からホストおよび EC2 クラウドインスタンスの VM スキャンを自動化

DevOps チームは、‘ Qualys VM Jenkins プラグイン ’ を使用して、Jenkins からホストおよび 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、セキュリティ上の欠陥を検出し除去するための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が実現します。『Jenkins Plugin for VM User Guide』を参照してください。



Golden AMI Pipeline

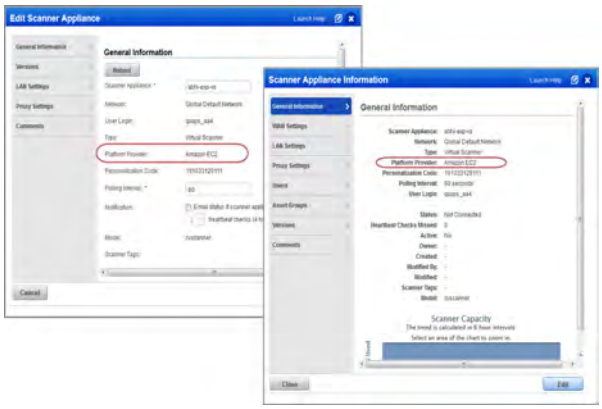
Golden Amazon Machine Image（AMI）を開発する際、DevOps チームは、連続的で自動化されたチェックを実行して、存在する脆弱性と誤設定を除去する必要があります。Qualys は Amazon と連携して、AWS 環境内に存在する強化 AMI のポートフォリオに対して継続的な評価を実行できるよう、AWS Golden Amazon Machine Image Pipeline の参照アーキテクチャを Qualys スキャナに統合しました。これにより、本番環境に進む前に、イメージ作成パイプラインにおける重大な脆弱性とコンプライアンスの問題を検出し修正できるようになります。



Qualys と Amazon の Golden AMI との統合の詳細については、「AWS Golden AMI Pipelines」、「動画シリーズ」を参照してください。

脆弱性を評価するための Golden AMI Pipeline と Qualys スキャナの統合に使用できるスクリプトも提供しています。詳細はこちらをご覧ください。

よくある質問

質問	回答
スキャン結果と EC2 のインスタンス ID について	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が作成されます。これにより、IP アドレスの変更が発生した場合であっても、アセットの追跡を継続することができます。スキャン中に IP アドレスの変更が検出され、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 のアセットインベントリには新しい IP アドレスが表示されます。
EC2 スキャンジョブでは、終了した EC2 インスタンスをどのように扱いますか	Qualys VM/VMDR または Qualys PC から開始されて、終了のステータスとなったすべての EC2 インスタンスは、EC2 スキャンから自動的に除外されます。そのため、終了した EC2 インスタンスのスキャンは行われません。オンデマンドで EC2 スキャンを開始した後に表示される「Launch EC2 Scan Preview」には、終了したインスタンスが表示されます。その理由は、インスタンスの除外は、スキャンジョブが Scanner Appliance に送信された後で行われるためです。
EC2 スキャンに必要なユーザパーミッションは何ですか	マネージャとユニットマネージャは、各自の Qualys ライセンスに従って、Qualys VM/VMDR および Qualys PC を使用した EC2 スキャンの開始、スケジュール、管理を行うことができます。 Qualys VM/VMDR - EC2 アセット上での脆弱性スキャンの実行 - Virtual 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 アセット上でのコンプライアンススキャンの実行 - Virtual 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 ユニットマネージャの要件 : マネージャは、アセットグループからユニットマネージャのビジネスユニットに EC2 環境の IP を追加する必要があります。マネージャは、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を、ユニットマネージャのビジネスユニットにあるアセットグループに追加する必要があります。
Virtual Scanner Appliance でプラットフォームプロバイダ情報を表示する方法	Amazon EC2（または他のクラウドプラットフォーム）に配置された Virtual Scanner Appliance のプラットフォームプロバイダ情報は、Qualys アカウント内に表示されます。この情報は、「Scans」→「Appliances」でアプライアンスの表示または編集時に、「General Information」セクションに表示されます。 

質問	回答
接続に関するトラブルシューティング	Qualys Scanner Appliance は、HTTPS を使用して Qualys クラウドプラットフォームに常時接続されている必要があります。アプライアンスを適切に動作させるには、接続に関する問題を解決してください。 スキャナと Qualys クラウドプラットフォームの間にネットワークの断絶があると、通信失敗のメッセージが表示されます。通信の障害が発生する理由としては、ローカルネットワークの停止、何らかの理由によるインターネット接続の切断、またはスキャナと Qualys クラウドプラットフォームとの間にあるいずれかのネットワークデバイスの停止などが考えられます。 ネットワークエラーのメッセージは、Scanner Appliance が Qualys クラウドプラットフォームへの接続を試みて失敗したことを示します。トラブルシューティングを容易にするために、エラーコードと説明が表示されます。エラーは、プロキシサーバと Qualys クラウドプラットフォームとの接続エラーが関係していることがあります。 Qualys クラウドプラットフォームは接続性チェックの結果と Amazon EC2 System Console の全般的な個人向けプロセスを記録しています。 「No connectivity to qualysguard.qualys.com - please fix.」というメッセージが表示された場合、VPN ネットワーク ACL とセキュリティグループで発信 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アクセス可能で、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可能であることを確認します。