コンテナセキュリティ
ユーザーガイド

2023 年 7 月 25 日

Qualys, Inc.

919 E Hillsdale Blvd , 4th Floor

Foster City, CA 94404

1 (650) 801 6100

目次

このガイドについて

Qualys Container Security へようこそ。Qualys Cloud Security Platform を使用して、イメージ、コンテナ、Docker ホストなどのコンテナ環境を保護するための 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、最も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 時間体制でサポートします。www.qualys.com/support/ でオンラインサポート情報にアクセスし ます。

コンテナセキュリティドキュメントについて

このドキュメントでは、Qualys Container Security UI を使用して、イメージ、コンテナ、およびレジストリの脆弱性を監視する方法について説明します。

MAC、CoreOS、およびさまざまなオーケストレーターとクラウド環境へのセンサーの展開については、以下を参照してください。

Qualys Container Sensor Deployment Guide

Container Security API の使用方法については、以下を参照してください。

Qualys Container Security API Guide

CI/CD 環境でのセンサーの展開については、以下を参照してください。

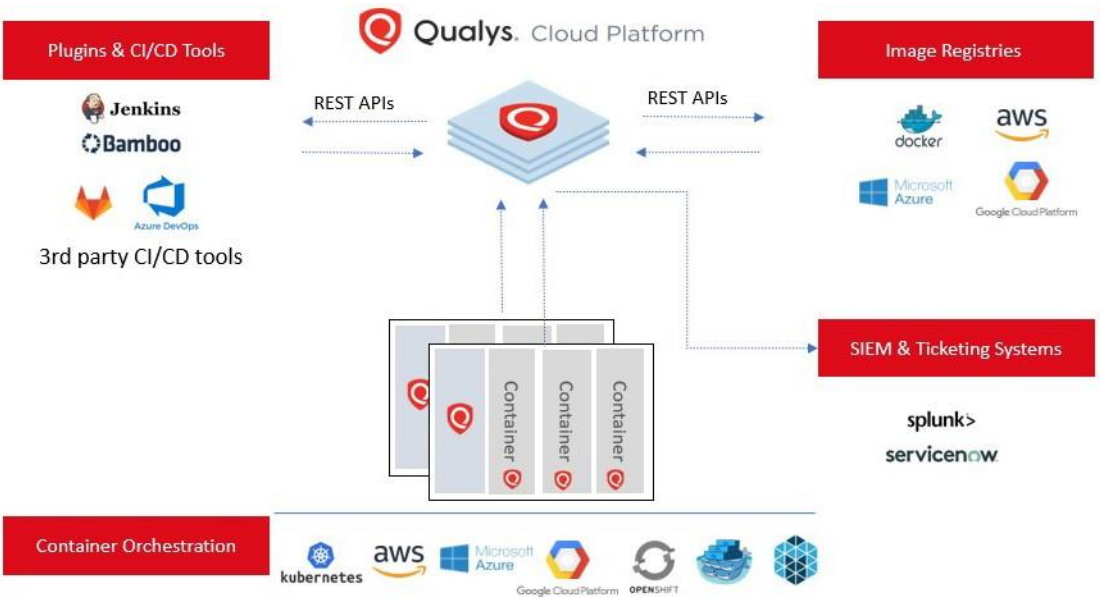
Qualys Container Scanning Connector for Jenkins

Qualys Container Scanning Connector for Bamboo

Qualys Container Scanning Connector for Azure DevOps

コンテナセキュリティの概要

Qualys Container Security は、コンテナ環境の検出、追跡、および継続的な保護を提供します。これにより、DevOps パイプライン内のイメージとコンテナの脆弱性管理、クラウド環境とオンプレミス環境にわたるデプロイメントに対応します。

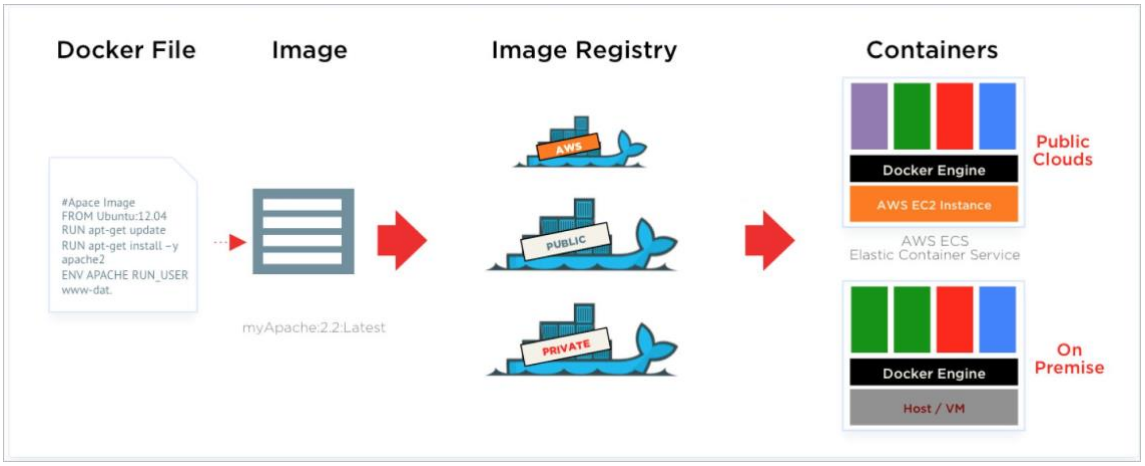


このバージョンでは、Qualys Container Security 下記の機能をサポートします。

- コンテナ環境の検出、インベントリ、およびほぼリアルタイムの追跡
- イメージとコンテナの脆弱性分析
- レジストリの脆弱性分析
- イメージとコンテナのコンプライアンス評価
- API を使用した CI/CD パイプラインとの統合 (DevOps フロー)

- Container Sensor の使用 – ネイティブコンテナサポートを提供し、Docker イメージとして配布

概念と用語



Docker イメージ

Docker イメージは読み取り専用のテンプレートです。たとえば、イメージには、Apache と Web アプリケーションがインストールされた Ubuntu オペレーティングシステムを含めることができます。
イメージは、Docker コンテナの作成に使用されます。Docker では、新しいイメージを構築したり、既存のイメージを更新したりするための簡単な方法を提供したり、他のユーザーが既に作成した Docker イメージをダウンロードしたりできます。Docker イメージは、Docker のビルドコンポーネントです。

イメージは、コンテナ内のアプリケーション コードやランタイム構成設定など、実行時のコンテナの静的な仕様です。Docker イメージには読み取り専用のレイヤーが含まれているため、イメージが作成されると変更されることはありません。

イメージは、イメージ ID と、イメージ UUID と呼ばれる Qualys によって生成された一意の識別子を使用して、Qualys コンテナ セキュリティ モジュール内で追跡されます。

Docker レジストリ

Docker レジストリはイメージを保持します。これらは、イメージをアップロードまたはダウンロードするパブリックストアまたはプライベートストアです。それらはあなたが使用するための既存のイメージの膨大なコレクションを提供します。自分で作成したイメージや、他のユーザーが以前に作成したイメージを使用することもできます。Docker レジストリは、Docker の配布コンポーネントです。スキャンでサポートされているパブリックレジストリとプライベートレジストリについては、「レジストリスキャン」を参照してください。インストゥルメンテーションのサポートについては、「コンテナランタイムセキュリティ」を参照してください。

Docker コンテナ

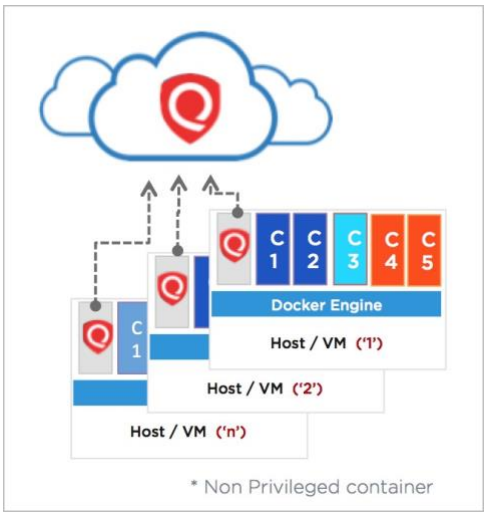
Docker コンテナはディレクトリに似ています。Docker コンテナには、アプリケーションの実行に必要なものがすべて含まれています。各コンテナは、Docker イメージから作成されます。Docker コンテナは、実行、起動、停止、移動、削除が可能です。各コンテナは、分離された安全なアプリケーションプラットフォームです。Docker コンテナは、Docker の実行コンポーネントです。

実行中の Docker コンテナは、イメージのインスタンス化です。同じイメージから派生したコンテナは、アプリケーション コードとランタイムの依存関係の点で互いに同じです。ただし、読み取り専用のイメージとは異なり、実行中の各コンテナには、読み取り専用コンテンツの上に書き込み可能なレイヤー (コンテナ レイヤー) が含まれています。データやファイルへの書き込みや更新など、ランタイムの変更は、コンテナレイヤーにのみ保存されます。したがって、同じ基になるイメージを共有する複数の同時実行コンテナは、異なるコンテナ レイヤーを持つ可能性があります。

コンテナは、コンテナ ID と、コンテナ UUID と呼ばれる Qualys によって生成された一意の識別子を使用して、Qualys コンテナ セキュリティ モジュール内で追跡されます。

Docker ホスト

ContainerD、CRI-O、Docker Daemon 上で実行され、コンテナとイメージをホストするホストまたはサーバー。Qualys はそれらをホストアセットとして追跡し、ホストの IP アドレス、DNS、その他の属性を含むメタデータを収集します。Qualys のホストは、一意の識別子 Host UUID によって識別されます。UUID は、Agent または Scanner Appliance による認証付きスキャンによって、/usr/local/qualys ディレクトリの下のマーカーファイルにも保存されます。



Qualys コンテナセンサー

Qualys Container Sensor は、Docker 環境をネイティブにサポートするように設計されています。センサーは Docker イメージとしてパッケージ化され提供されます。イメージをダウンロードし、ホスト上の他のアプリケーションコンテナと一緒にコンテナとしてデプロイします。

センサーは Docker ベースで、データセンターや AWS ECS、Azure Container Service、Google Container Service などのクラウド環境のホストにデプロイできます。Sensor は現在、CentOS、Ubuntu、RHEL、Debian などの Linux オペレーティングシステムでのみサポートされており、バージョン 1.12 以降の Docker デーモンを使用可能にする必要があります。

Docker ベースであるため、センサーは他のアプリケーションコンテナと同様に、Kubernetes、Mesos、Docker Swarm などのオーケストレーションツール環境にデプロイできます。

インストール時に、センサーはデプロイされたホスト上のイメージとコンテナを自動的に検出し、それらの脆弱性分析を提供し、さらにホスト上の Docker 関連イベントを監視および報告します。センサーはコンプライアンス評価も実行します。センサー コンテナは、非特権モードで実行されます。ファイルを保存およびキャッシュするための永続ストレージが必要です。

現在、センサーはイメージとコンテナのみをスキャンします。ホストをスキャンするには、Qualys Cloud Agents または Qualys Virtual Scanner Appliance を使用したスキャンが必要です。

センサー モード(一般、レジストリ、CI/CD)については、『Qualys Container Security センサー導入ガイド』を参照してください。

Container Security はどのようなデータを収集しますか?

Qualys コンテナ セキュリティ センサーは、環境内のイメージとコンテナに関する次の情報を取得します。

すべてのコンテナを一覧表示する docker ps などのコマンドにより、環境内の**イメージとコンテナのインベントリ** を取得します。

docker inspect や docker info などのコマンドにより、イメージとコンテナに関する**メタデータ情報**で、Docker オブジェクトに関する低レベルの情報を取得します。

作成、開始、強制終了、プッシュ、プルなどの Docker イベントに関する Docker ホストからのイメージとコンテナに関する**イベント情報**を取得します。

イメージとコンテナで見つかった**脆弱性**。これらは、イメージとコンテナの脆弱性情報を識別するために実行される脆弱性管理マニフェストの出力です。主に、ソフトウェアパッケージのリスト、実行中のサービス、ポートなどです。例えば、パッケージ マネージャーは rpm -qa、npm の

ように出力します。また、さまざまな Linux ディストリビューション(CentOS、Ubuntu、CoreOS など)と、Python、NodeJS、Ruby などのイメージでサポートされています。

OCI 準拠のイメージ、実行中のコンテナの**コンプライアンス構成**。CIS Docker ベンチマークのコントロールのサブセットをサポートしており、コンテナとイメージの実行に適用できます。お客様は、実行中のコンテナとイメージの構成リスクを評価し、Qualys の調査結果に基づいて適切に修正できます。コンテナやイメージのコンプライアンススキャンは、お客様に対して透過的であり、脆弱性スキャン機能と同様にリアルタイムのクラウドネイティブな方法で機能します。

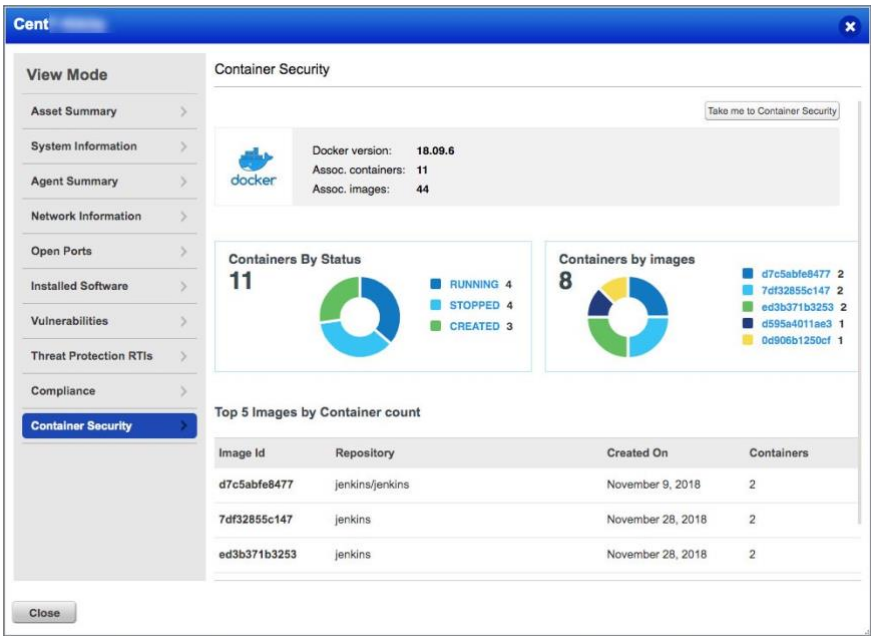
Container Security 無料版

Qualys は、Container Security が提供するものを見ることができるように、Container Security App の無料バージョンを導入しました。無料版では、環境内のコンテナとイメージのビューが提供されます。これらのイメージとコンテナの脆弱性をスキャンする場合は、Container Security の有料サブスクリプションにアップグレードする必要があります。

Container Security は、ホストに Docker が含まれている場合、次のいずれかのソースからイメージとコンテナの情報を取得します。

クラウドエージェント/スキャナー

ホストまたはスキャナーに(認証済みスキャンを介して)インストールされた Cloud Agent は、ホストに存在するコンテナとイメージのリストを取得し、この情報を AssetView アプリの[**Asset Details**]>[**Container Security**]ペインで各アセットに提供します。



[**Take me to Container Security**] オプションをクリックして、アカウントの Container Security 無料バージョンを有効にします。

Container Security アプリには、イメージとコンテナのメタデータが表示されますが、脆弱性情報は表示されません。イメージとコンテナの脆弱性をスキャンするには、有料サブスクリプションにアップグレードする必要があります。詳細については、「ホスト」を参照してください。

コンテナセンサー

ホストに Container Sensor をインストールすると、Docker Hub からすべての公式イメージの脆弱性情報が取得され、アカウント内のアセットにインストールされている最初の 10 個の汎用センサーが取得されます (CI/CD およびレジストリ スキャン用のセンサーは含まれません)。試用版または完全版 (有料) サブスクリプションにアップグレードすると、この制限が解除されます。

API サポート

コンテナ、イメージ、センサーを一覧表示し、コンテナ、イメージ、センサーの詳細を取得する API は、Container Security Free で使用できます。有料サブスクリプションにアップグレードすると、すべての Container Security API にアクセスできます。『Qualys Container Security API ガイド』を参照してください。

コンテナランタイムセキュリティ

Container Runtime Security(CRS)は、実行中のコンテナに対して、実行時の振る舞いの可視化と適用機能を提供します。これにより、お客様は、セキュリティのベストプラクティスの適用、ファイルアクセスの監視、ネットワークアクセス制御など、コンテナを実行するためのさまざまなユースケースに対応できます。

CRS では、コンテナイメージにプローブを挿入する Qualys コンテナランタイムインストゥルメンテーションを使用してコンテナイメージをインストゥルメンテーションする必要があります。お客様は、インストゥルメント化されたイメージ、コンテナの動作、可視性を管理する詳細なポリシーを持つコンテナを構成できます。これらのランタイム適用ポリシー(ランタイムイベント)に基づいて、UI、API を介してバックエンドから取得したテレメトリを表示できます。

CRS は現在、Linux OS ベースのコンテナでのみサポートされています。

CRS ドキュメント

CRS User Guide | CRS API Guide

データ保持ポリシー

センサー、コンテナ、およびイベントのデータ保持ポリシーを実装しました。データ保持ポリシーは、データが保持される期間が指定されたデータ保持ポリシー期間を超えた場合に、Qualys Container Sensor プラットフォームからデータを削除します。

データ保持期間

データ保持期間は、次の表に示すデフォルト値で構成されます。これらのデータ保持ポリシーに従って削除される前に、API を使用してデータをエクスポートしてください。

データタイプ	既定の保持期間の値 (日数)
Sensor	390 (approx. 13 months)
Container	390 (approx. 13 months)
Event (Behavioral)	3
Event (Standard)	7

なぜデータ保持ポリシーを導入したのですか?

クラウドプラットフォーム全体でデータ保持ポリシーを標準化するにあたり、センサーとコンテナのポリシーを更新しています。統一されたデータ保持ポリシーにより、常に最新のデータが利用可能になり、データの関連性が向上し、システム全体のパフォーマンスが最適化されます。

保持期間が経過すると、データにアクセスできるようになりますか?

いいえ、保持ポリシーに従ってデータがパージされると、データは復元できません。Container Security のデータ保持ポリシーについてご不明な点がございましたら、Qualys サポートにお問い合わせください。

データ保持ポリシーをカスタマイズできますか?

はい、イメージ、コンテナ、センサーの保持ポリシーをカスタマイズできます。保持ポリシーのオプションをカスタマイズするには、［構成］>［全般］に移動します。

詳細については、「リンク」を参照してください。

はじめに

この章では、Container Security Sensor のインストールの概要について説明します。

MAC、CoreOS、およびさまざまなオーケストレータおよびクラウド環境へのセンサーの展開については、『Qualys Container Sensor Deployment Guide』を参照してください。

コンテナ・セキュリティ・ドキュメントについてを参照してください。

Qualys サブスクリプションとモジュールが必要

アカウントで「コンテナセキュリティ」(CS)モジュールを有効にする必要があります。また、コンテナを実行するホストの脆弱性を取得するには、Scanner Appliance または Cloud Agent を使用して脆弱性管理(VM)を有効にする必要があります。

システムサポート

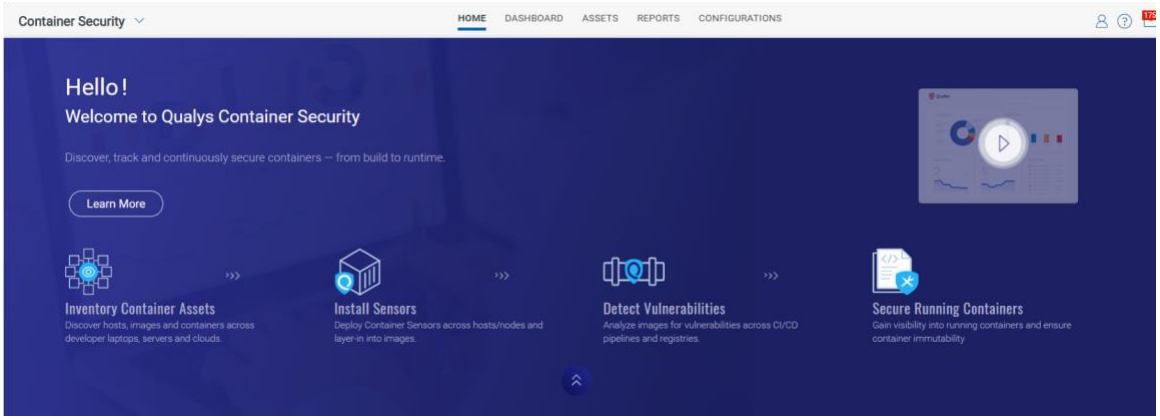
サポートされているシステムのリストについては、『Qualys Container Security Sensor Deployment Guide』を参照してください。

Container Sensor のデプロイ

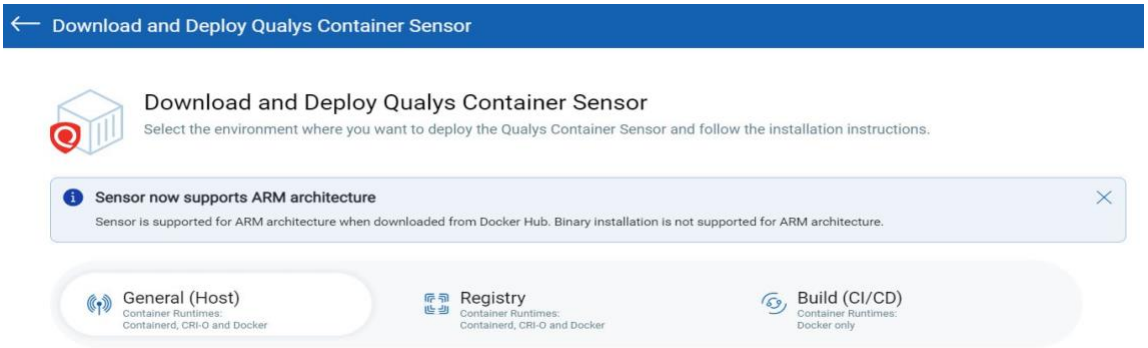
重要: センサーの展開は、1 つのホスト/ノード上の 1 つのモードに 1 つのセンサーです。複数のセンサーまたは複数のセンサーを別のモードで展開することはサポートされていません。

さあ、始めましょう。　ユーザー クレデンシャルを使用して Qualys ポータルにログインします。モジュールピッカーから [Container Security] を選択します。

初めてのユーザーは、はじめにページに直接アクセスします。



Configurations > Sensors に移動し、Download Sensor をクリックして センサーの tar ファイルをダウンロードします。さまざまなセンサータイプを確認できます。



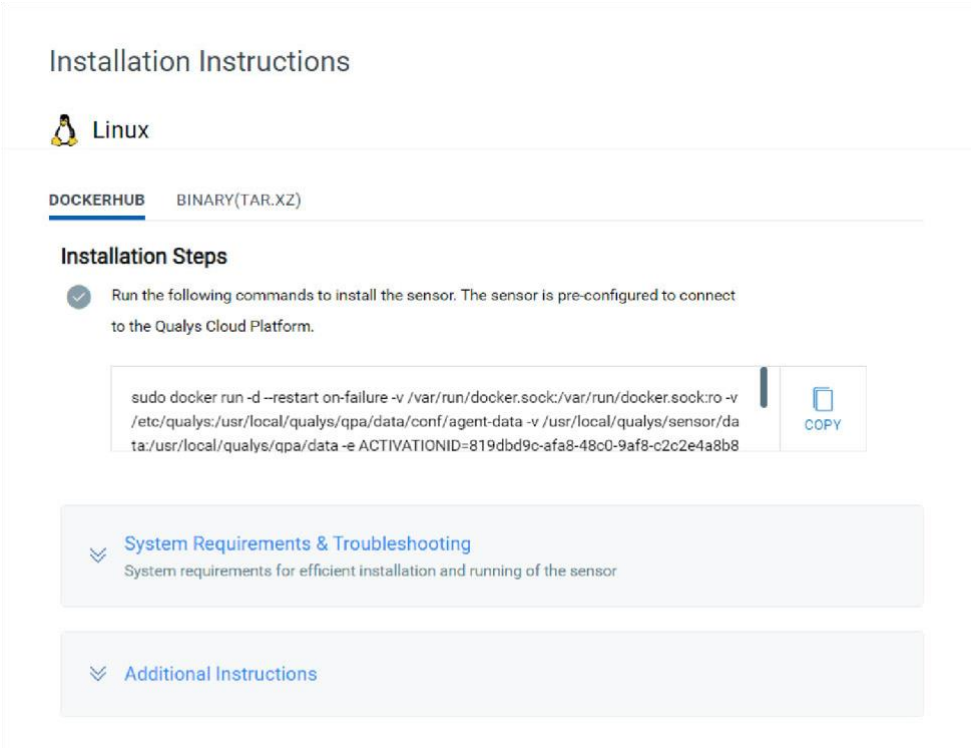
General (Host) Sensor: レジストリ/ビルド (CI/CD) 以外のホストをスキャンします。

Registry Sensor: レジストリ(パブリック/プライベート)内のイメージをスキャンします。

Build (CI/CD) Sensor: CI/CD パイプライン (Jenkins / Bamboo) でイメージをスキャンします。

レジストリの場合は、インストールコマンドに --registry-sensor or -r　を使用し、

CI/CD の場合は、install コマンドに --cicd-deployed-sensor or -c　を使用します。



QualysContainerSensor.tar.xz ファイルをダウンロードし、Docker ホストの画面から直接生成されたコマンドを実行します。センサーをインストールするための要件に注意してください。センサーにはホストに最低 1 GB の永続ストレージが必要です。

「installsensor.sh」スクリプトのコマンドラインパラメータの詳細については、『Qualys Container Security Sensor 導入ガイド』の「Deploying Container Sensor」の項を参照してください。

プロキシのサポート

インストール スクリプトは、プロキシ構成を要求します。IP アドレス/FQDN とポート番号、およびプロキシ証明書ファイルのパスを指定する必要があります。例えば、

```
Do you want connection via Proxy [y/N]: y

Enter Https Proxy settings [<IP Address>:<Port #>]: 10.xxx.xx.xx:3xxx

Enter Https Proxy certificate file path: /etc/qualys/cloudagent/cert/ca-bundle.crt
```

プロキシ サーバは、HTTPS ポート 443 経由で Qualys Cloud Platform (または Qualys プライベート クラウド プラットフォーム) へのアクセスを提供する必要があります。ホストがアクセスする必要がある Qualys プラットフォーム(POD URL)については、以下を参照してください。

ホストがアクセスする必要がある Qualys プラットフォーム(POD URL)

使用する Qualys URL は、アカウントが配置されている Qualys プラットフォームによって異なります。 Qualys プラットフォームを特定し、Container Security Server の URL を取得するには、ここをクリックしてください。

POD URL 値

プラットフォームの「コンテナセキュリティサーバ URL」(上記のリンクにあります)は、センサーをデプロイするときに、コンテナセキュリティセンサーコマンドと設定 yaml ファイルで POD_URL 変数に指定する必要がある URL です。

センサーのネットワーク構成

センサーには、Qualys の URL と、Qualys との通信に必要なサブスクリプションの詳細が事前設定されています。センサーが Qualys と通信するには、ネットワーク設定とファイアウォールがポート 443 経由で Qualys ドメインにアクセスできるようにする必要があります。

センサーが正常にインストールされると、センサーはコンテナセキュリティ UI の Configurations >Sensors に一覧表示され、バージョン、ステータスなどを確認したり、詳細にアクセスしたりできます。さらに、UI からセンサーをダウンロードすることもできます。

Docker イメージの静的スキャン

センサーは、docker イメージにシェルがない場合に、現在の動的スキャンへのフォールバック メカニズムとして Docker イメージの静的スキャンを実行します。静的スキャンは、シェルのない Google ディストリビューションイメージに対しても実行されます。静的スキャンは、シェルを持つ Docker コンテナまたは Docker イメージでは実行されません。

静的スキャンは、インストールされているソフトウェアのリストを Docker イメージ・ファイル・システムから収集して、Docker イメージの脆弱性を検出します。インストールされているソフトウェアの一覧は、パッケージ マネージャーのメタデータ ファイルから取得されます。サポートされているパッケージマネージャーは、RPM、DPKG、および Alpine です。

センサーが実行されているホストにシェルのない大きなイメージがある場合、ディスク容量の要件が最小要件の 1 GB を超える可能性があります。

ユーザーと権限

Qualys Container Security アプリケーションは、ロールベースのアクセス制御(RBAC)モデルを使用して、コンテナセキュリティ機能へのアクセスを制御します。RBAC では、各ユーザーに事前定

義されたユーザー ロールが割り当てられ、ユーザーが UI と API で実行できるアクションが決まります。

ユーザー ロールについて

Manager ユーザー(完全な権限とスコープを持つスーパーユーザー)は、管理ユーティリティにアクセスでき、すべてのロールを割り当て、ユーザーを追加および管理し、カスタムロールを作成し、ユーザーにロールを割り当てることができます。新しい顧客サブスクリプションの最初のユーザーは Manager ユーザーです。

コンテナセキュリティには、次の事前定義されたロールがあります。これらのロールは、Container Security モジュール専用です。他のモジュールで定義されているロールは、コンテナセキュリティで定義されているロールと相関関係がありません。

CS Manager: CS Manager には、すべてのコンテナ セキュリティ権限があり、コンテナ セキュリティ UI と API ですべてのアクションを実行できます。Container Security 1.17 リリースより前に存在していたすべての Container Security ユーザーには、CS Manager ロールが自動的に割り当てられ、すべてのアクションを実行できます。

CS ユーザー: CS ユーザーロールには、コンテナ セキュリティ UI にアクセスする権限のみがあり、他の権限は割り当てられていません。

注: このロールは、Container Security 1.17 以降に作成された新しい顧客サブスクリプションでは使用できません。

役割と権限を表示する方法

マネージャは、管理ユーティリティからユーザーの役割と権限を表示できます。ヘルプが必要な場合は、Qualys Administration Utility のヘルプを参照してください。

既存のユーザーからアクセス許可を削除する方法

Container Security 1.17 リリースより前に存在していたすべてのユーザーは、すべての Container Security 権限を付与する「CS Manager」ロールを自動的に取得します。特定のユーザーの権限を制限する場合は、カスタムロールを作成し、ユーザーに付与する権限のみを選択する必要があります。

管理ユーティリティの「ユーザー」>「ユーザー管理」タブからユーザー・アカウントを編集します。「CS Manager」ロールは、ユーザーにすべての権限を付与するため、ユーザーから削除し、新しいカスタム ロールをユーザーに割り当てます。

新しいユーザーを追加する方法

すべてのマネージャは、新しいユーザーを追加し、ロールと権限を割り当てることができます。ユーザーは、管理ユーティリティから追加できます。開始する前に、新しいユーザーに付与する

ロールとアクセス許可について考えます。詳細については、「ユーザーと権限」を参照してください。

次の手順に従って、ユーザーを追加します。

1) アプリケーションピッカーの **Utilities** で **Administration** を選択します。

2) **Users > User Management** タブに移動します。

3) Create User メニューから、次のオプションのいずれかを選択します。

Create Reader User – ユーザーには、VM ユーザー、閲覧者、レポート閲覧者のロールが自動的に割り当てられます。ユーザーには、コンテナセキュリティのロール/権限が自動的に割り当てられることはありません。CS ロールを追加するには、ユーザー アカウントを編集する必要があります。

Create manager User – ユーザーには、すべてのロールが割り当てられ、完全な権限とスコープが割り当てられます。マネージャ ユーザーは、管理ユーティリティにアクセスできます。

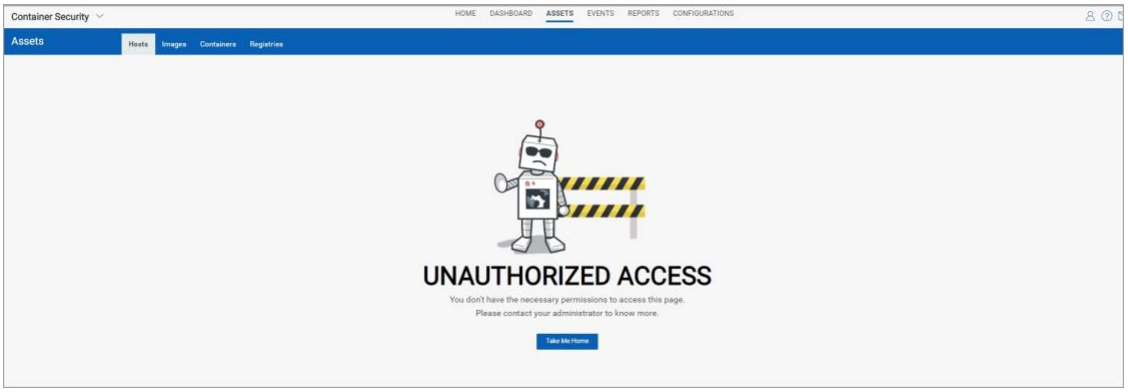
4) ユーザー設定を定義します。設定のヘルプについては、右上隅にある [Launch Help] リンクをクリックしてください。ユーザーを追加すると、ログイン手順が記載されたウェルカムメールが送信されます。

5) Manager 以外のユーザーの場合は、ユーザーの設定を編集して、ユーザーに Container Security のロールと権限を割り当てる必要があります。User Managment タブで、Quick Actions メニューから Edit を選択します。**Roles and Scopes** タブに移動して、定義済みのロールを割り当てます。

ユーザーがアクションを実行する権限を持っていない場合

ユーザーに特定の権限が付与されていない場合、ユーザーは UI または API から関連するアクションを実行できません。

ユーザーにオブジェクトに対するリスト権限がない場合、ユーザーは UI で関連データリストを表示したり、API からリストを取得したりすることはできません。UI では、リストを表示する権限がない場合、**UNAUTHORIZED ACCESS** メッセージが表示されます。次の例では、ユーザーにはホストの一覧表示権限がありません。



ユーザーがリスト権限を持っていても、作成、更新、削除などの他の権限を持っていない場合、リストはユーザーに表示されますが、アクションのボタンまたはメニューオプションは表示されません。たとえば、ユーザーに [レジストリの作成] アクセス許可がない場合、ユーザーには [新しいレジストリ] ボタンが表示されず、API からレジストリを作成できません。

コンテナセットの保護

アセットインベントリ

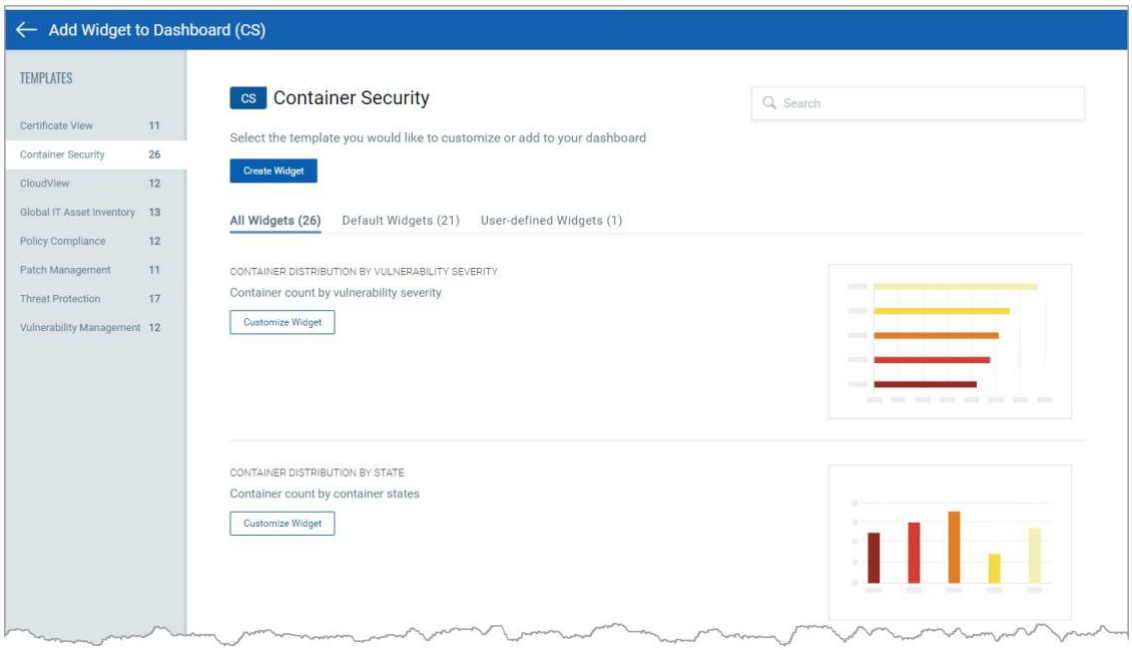
センサーをインストールすると、ホスト上に存在するイメージとコンテナについて、ホストが自動的にスキャンされます。インベントリとインベントリのメタデータが Qualys ポータルにプッシュされます。

統合ダッシュボード

ダッシュボードは、コンテナ環境の資産を可視化し、脅威にさらされていることを確認し、保存された検索を活用し、脆弱性の優先度を迅速に修正するのに役立ちます。

Unified Dashboard(UD)と Container Security を統合しました。UD は、すべての Qualys アプリケーションからの情報を 1 か所に集めて視覚化します。UD は、強力な新しいダッシュボードフレームワークとプラットフォームサービスを提供し、既存のダッシュボード機能を強化するために他のすべての製品で使用および使用されます。

Qualys が提供するデフォルトのコンテナセキュリティダッシュボードを使用するか、ウィジェットを簡単に設定して、他のモジュール/アプリケーションから情報を取得してダッシュボードに追加できます。ダッシュボードをいくつでも追加して、ビューをカスタマイズすることもできます。ウィジェット、ダッシュボード、テンプレートなどの作成については、統合ダッシュボードのオンラインヘルプを参照してください。



アセットの詳細

[アセット] セクションには、検出されたイメージとコンテナが、ポート、ネットワーク、サービス、ユーザー、インストールされているソフトウェアなどのメタデータ情報とともに一覧表示されます。アセットは、イメージに関連付けられたコンテナやホスト、同じ親イメージの他のコンテナなどの関連付けとともに一覧表示されます。ユーザーは、属性に基づいてイメージとコンテナを検索できます。

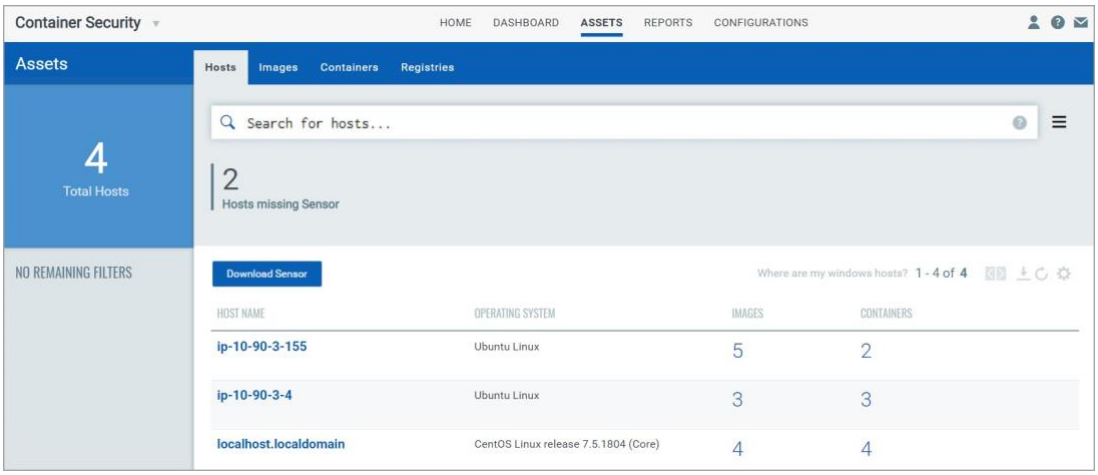
Jump to a section: Hosts | Images | Containers | Registries

Hosts

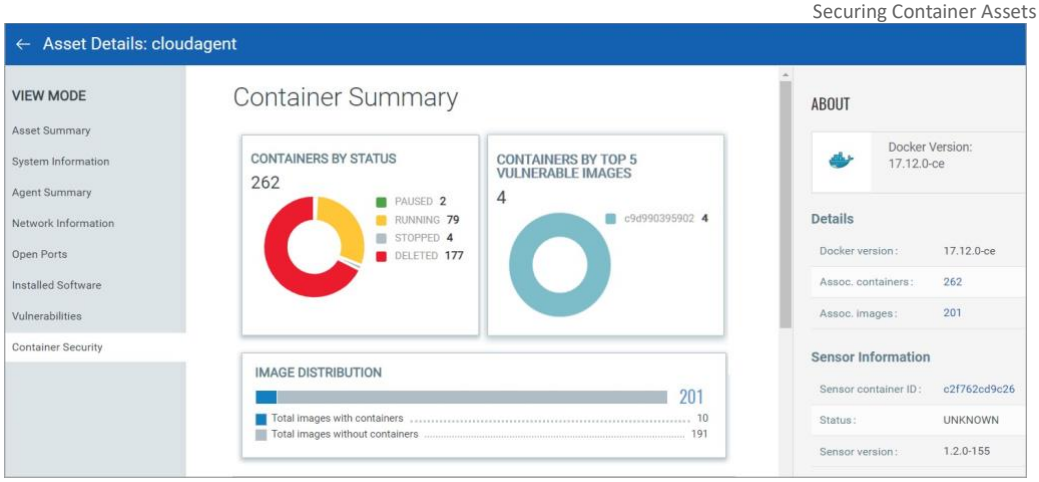
[**Assets > Hosts**] タブには、Qualys Cloud Agent や Qualys Network Scanner によって検出およびスキャンされたコンテナホストが表示されます。現在、Qualys コンテナ センサーによってのみ検出され、スキャンされたコンテナ ホストは、このリストに表示されません。これらには [Images] タブまたは [Containers] タブを使用することをお勧めします。さらに、Qualys コンテナ センサーは現在、Linux ベースのホスト OS と Mac OS のホストとクラスタのみをサポートしています。

リスト内のホストごとに、イメージとコンテナの数が表示されます。イメージとコンテナの詳細は、それぞれのタブで確認できます。

QQL 検索トークンを使用してホストを検索します。 検索トークンのリストについては、オンライン・ヘルプを参照してください。

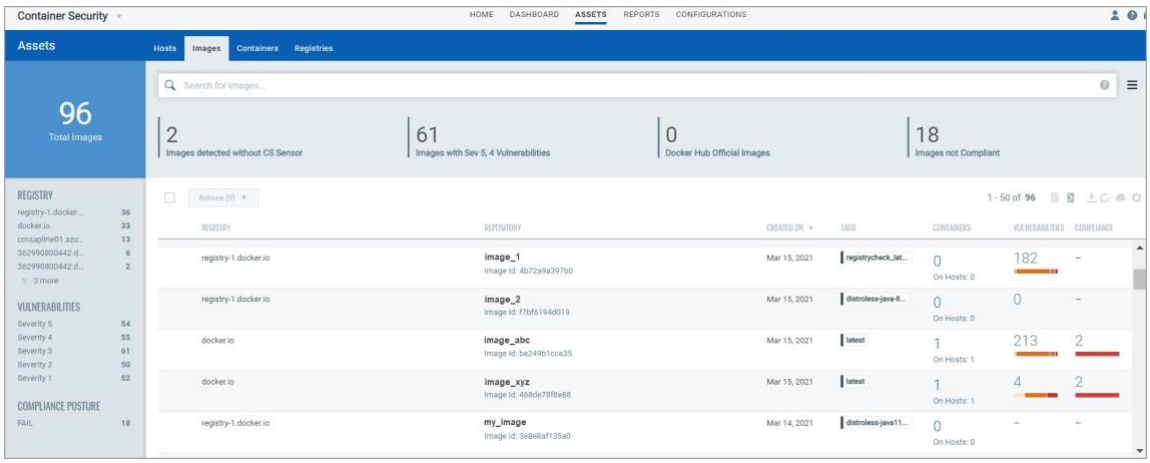


センサーの詳細ページからホストの詳細ページにアクセスします。[Asset Details] ビューには、センサーが展開されているホストに関する情報が表示されます。システム、ネットワーク、およびポート情報に加えて、アセットの詳細ビューには、ホストにインストールされているソフトウェア、存在する脆弱性、証明書、および脅威対策 RTI (Qualys TP アプリケーションが有効な場合) のリストも表示されます。[Container Security] パネルには、ホストにインストールされているすべてのコンテナ、そのステータス、およびコンテナの生成元のイメージが表示されます。



イメージ

「**アセット>イメージ**」タブには、検出されたイメージとそのメタデータ情報が表示されます。QQL 検索トークンを使用してイメージを検索します。検索トークンのリストについては 、オンライン・ヘルプを参照してください。

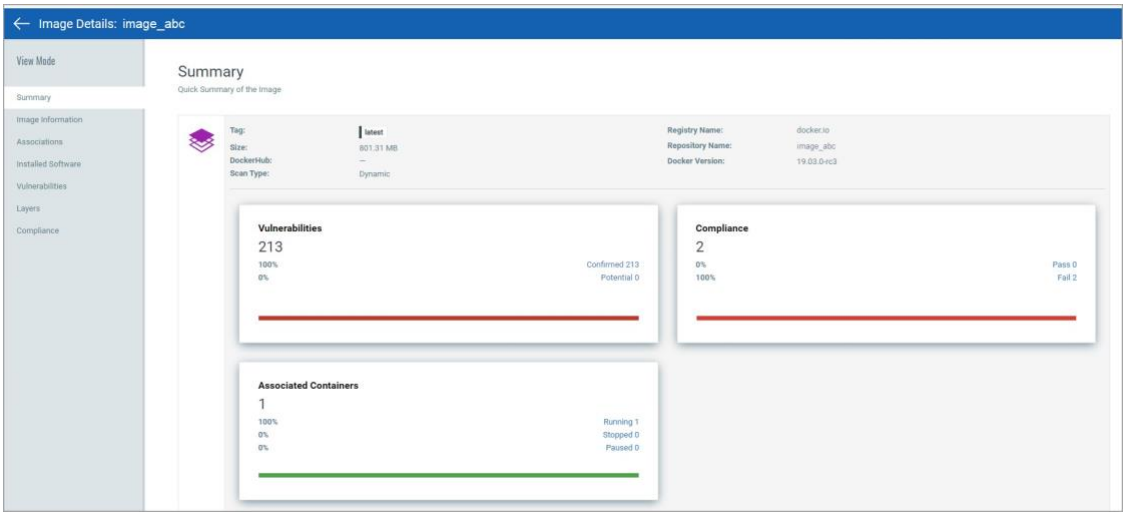


[クイックアクション] メニューから [タグの追加］を選択して、静的アセットタグをイメージに割り当てます。タグを追加するときに、新しいタグを作成するオプションがあります。また、割り当てられたタグを、選択したイメージに関連付けられているコンテナに渡すこともできます。

リスト内の任意のイメージの [クイック アクション] メニューから [詳細の表示] を選択して、イメージに関する包括的な情報を取得します。イメージ、コンテナ、ドリフトコンテナ、およびホストとの関連付けに関する詳細情報を表示できます。

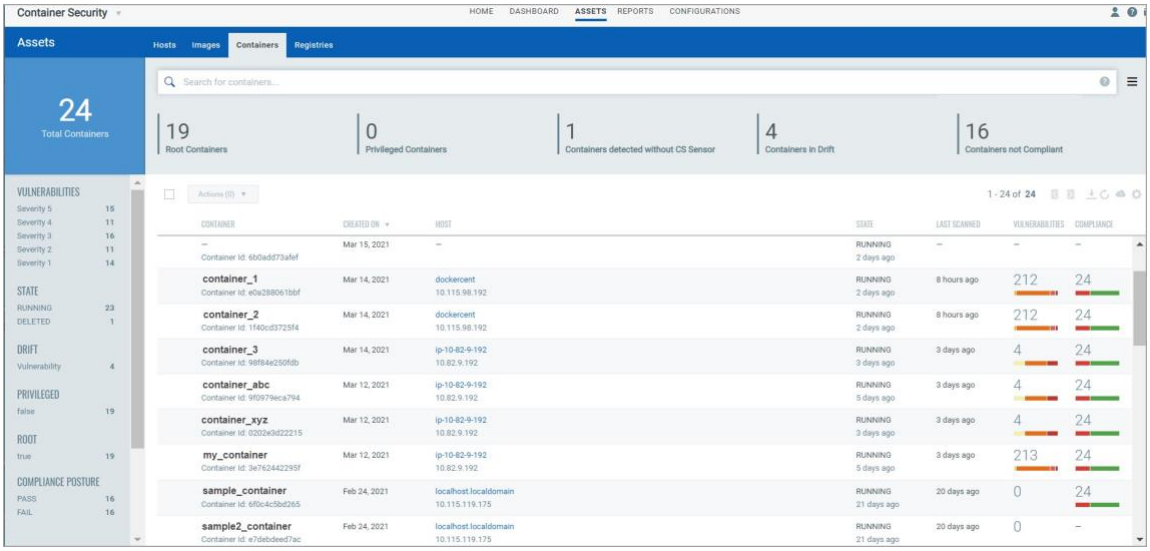
- 「インストールされているソフトウェア」セクションには、脆弱性のあるソフトウェアと、修正(パッチ)が利用可能なソフトウェアが表示されます。

- [脆弱性(Vulnerabilities)] セクションには、確認された脆弱性や潜在的な脆弱性などの脆弱性情報とその重大度が表示されます。脆弱性ごとに、脆弱性の経過時間(日数)が表示されます。経過時間は、Qualys が脆弱性を公開した時点から計算されます。
- [コンプライアンス] セクションには、スキャンされたコントロールの一覧とコントロールの詳細 (CID、重要度、ステートメント、カテゴリ、テクノロジ) が表示されます。
- 「レイヤー」セクションには、イメージを構成するレイヤーのリストが表示されます。



コンテナ

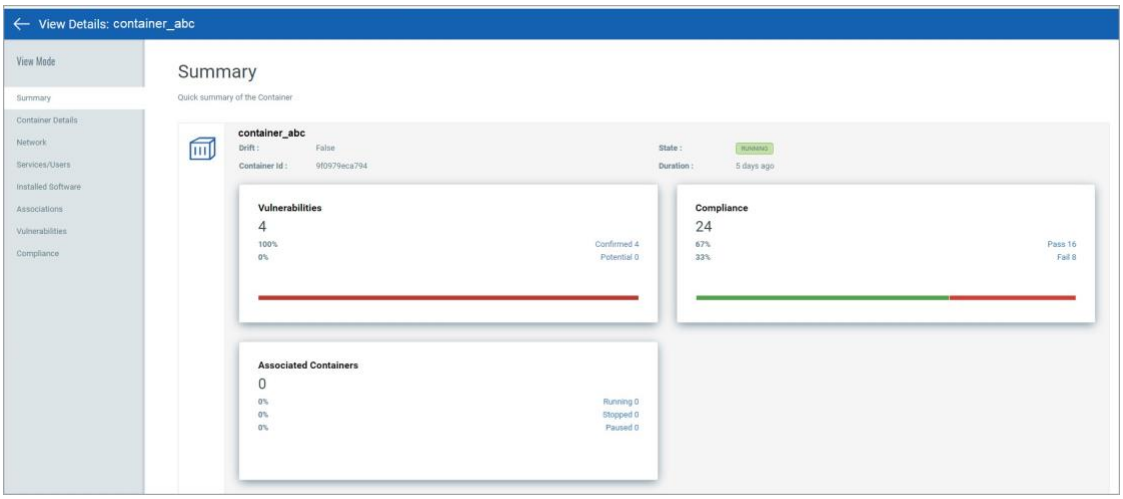
Assets > Containers タブには、検出されたコンテナとそのメタデータ情報が表示されます。QQL 検索トークンを使用してコンテナを検索します。 検索トークンのリストについては、オンライン・ヘルプを参照してください。



[クイックアクション] メニューから [タグの追加] を選択して、静的アセットタグをコンテナに割り当てます。また、割り当て中に新しいタグをその場で作成することもできます。

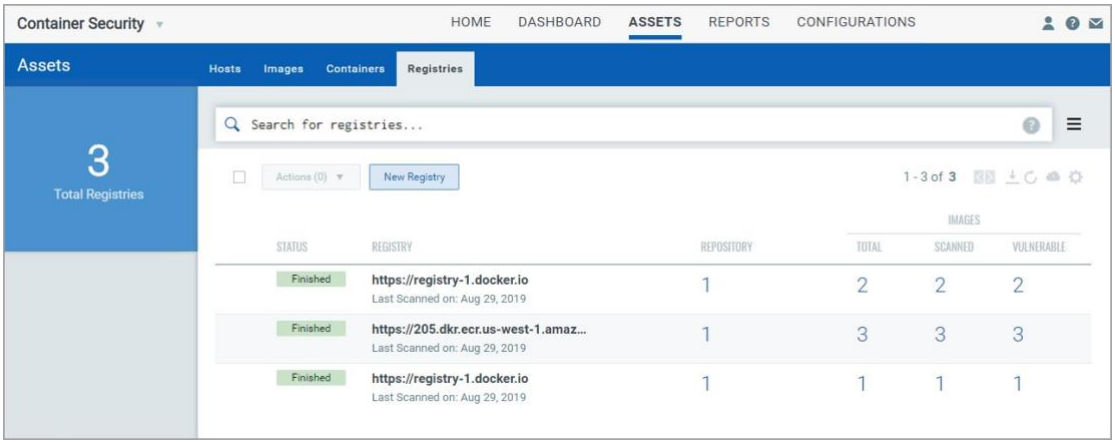
リスト内の任意のコンテナの「クイック・アクション」メニューから「詳細の表示」を選択して　、コンテナに関する包括的な情報を取得します。コンテナ、イメージとの関連付け、ドリフト コンテナ、およびホストに関する詳細情報を取得します。

- コンテナの「状態」は、Qualys センサーが Qualys Cloud Platform に報告する Docker イベント (exec_start、kill、destroy、stop)に基づいて更新されます。
- [サービス/ユーザー] セクションには、コンテナで使用可能なサービスと、コンテナに関連付けられているユーザーの一覧が表示されます。
- ［インストールされているソフトウェア］セクションには、脆弱性のあるソフトウェアと、修正(パッチ)が利用可能なソフトウェアが表示されます。
- [脆弱性(Vulnerabilities)] セクションには、確認された脆弱性や潜在的な脆弱性などの脆弱性情報とその重大度が表示されます。脆弱性ごとに、脆弱性の経過時間(日数)が表示されます。経過時間は、Qualys が脆弱性を公開した時点から計算されます。
- コンプライアンスは、コントロールの詳細 (CID、重要度、ステートメント、カテゴリ、テクノロジ) と共にスキャンされたコントロールの一覧を提供します。

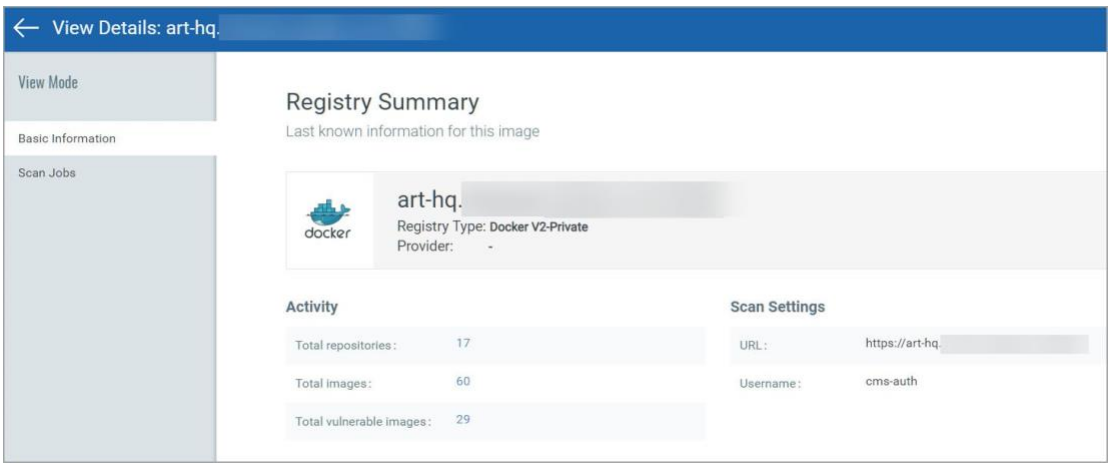


レジストリ

Assets >Registries タブには、アカウント内のレジストリが表示されます。QQL 検索トークンを使用してレジストリーを検索します。 検索トークンのリストについては、オンライン・ヘルプを参照してください。



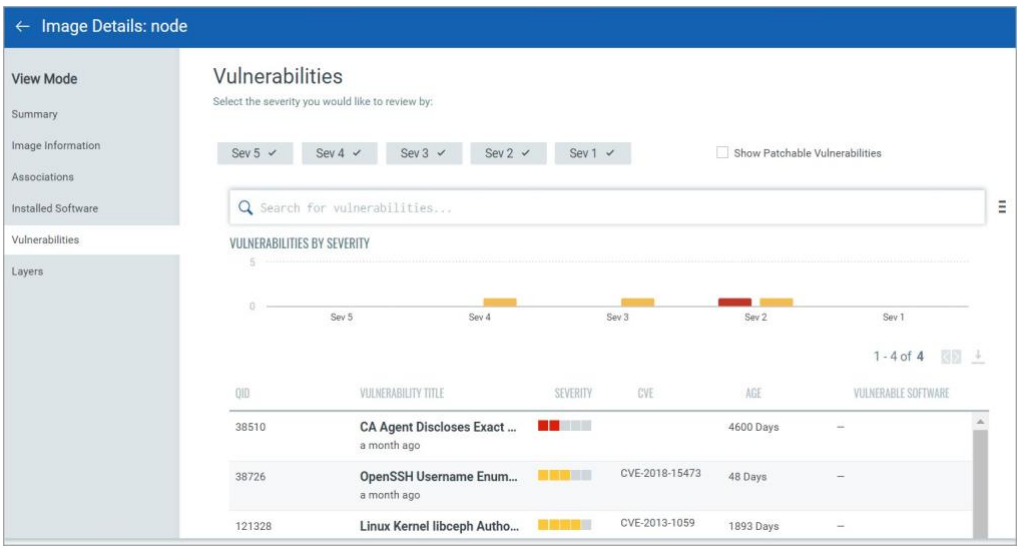
リスト内の任意のレジストリの「クイック・アクション」メニューから「詳細の表示」を選択して、レジストリに関する包括的な情報を取得します。レジストリに関する詳細情報（リポジトリの数、イメージの合計数、そのレジストリ内の脆弱なイメージの数）を表示できます。「スキャン・ジョブ」パネルには、そのレジストリー用に作成されたオンデマンド・ジョブと自動ジョブがリストされます。詳細については、「レジストリ スキャン」を参照してください。



Docker イメージの脆弱性スキャン

Docker イメージがスキャンされ、Qualys コンテナ センサーによって脆弱性の存在が確認されます。[イメージの詳細(Image Details)]の脆弱性パネルには、重大度が [脆弱性(Severity)] の脆弱性とその QID のリストが表示されます。「Show Patchable Vulnerabilities」を選択して、使用可能なパッチがある脆弱性を表示します。

Qualys は、静的分析ではなく、イメージを完全なエンティティとして見る非静的な方法で Docker イメージの脆弱性をスキャンします。このプロセスは、より一般的に使用される静的分析よりも効果的で、誤検知 (FP) が少なくなります。



Docker イメージは、開発者のラップトップ、ビルドシステム、イメージレジストリから、コンテナを実行している Docker ホストにキャッシュされる環境全体に分散されています。脆弱性をスキャンするには、ホスト資産にデプロイされたコンテナセンサーが必要です。

イメージのインベントリを取得し、脆弱性をスキャンするには、ホストにコンテナ センサーをデプロイします。 インストール手順とシステム要件については、「Container Sensor のデプロイ」を参照してください。

ローカル・ホストまたはラップトップ上

イメージのインベントリを取得し、脆弱性をスキャンするには、ローカルホストにコンテナセンサーをデプロイします。 インストール手順とシステム要件については、「Container Sensor のデプロイ」を参照してください。

センサーを Mac ラップトップに展開するには、追加のインストール手順があります - Qualys Container Security センサー導入ガイドの指示に従ってください。「コンテナ・セキュリティ・ドキュメントについて」を参照してください。

インストール時に、センサーはイメージを自動的に検出し、イメージのインベントリと脆弱性スキャンを提供します。

CI/CD パイプライン内

ビルド時にイメージの脆弱性を完全にチェックすることで、よりクリーンな運用環境を確保できます。Qualys Container Security は、Jenkins と Bamboo がビルド環境内のイメージの脆弱性分析を取得するためのプラグインを提供します。他のツールを使用している場合は、使用可能な REST API を使用して、イメージの脆弱性分析を実行できます。

まず、イメージが作成されているビルド ホストに Container Sensor をデプロイします。インストール時にセンサーは、検出された新しいイメージの脆弱性分析を自動的にトリガーします。API またはプラグインを使用して、イメージの脆弱性を探します。Jenkins または Bamboo 環境の場合、プラグインは脆弱性の詳細リストとその詳細をプラグイン内で直接提供し、オプションで Qualys サブスクリプションにアクセスして完全なレポートを表示できます。

レジストリ内

現在、Qualys コンテナ センサーは、分析を行うためにイメージを自動的にポーリングまたはプルしません。代わりに、レジストリからイメージをプルするように構成されたホストにセンサーを展開する必要があります。手動または cron を使用して、新しいイメージをホストにプルします。センサーは、新しいイメージを見つけるとすぐに自動分析を行います。API または Qualys ポータルを使用して、特定された脆弱性を照会します。

AWS Fargate(ECS)の場合

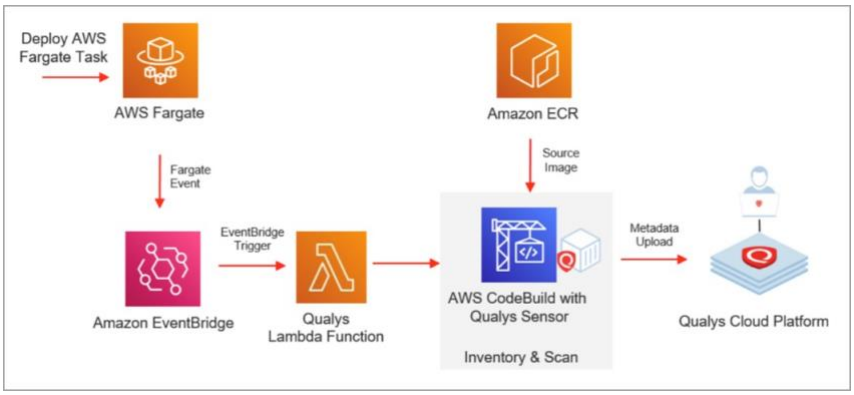
Qualys Container Security を使用して、AWS Fargate を保護できます。AWS Fargate は、Amazon Elastic Container Service (ECS) と連携するコンテナ用のサーバーレスコンピューティングエンジンです。この機能を使用すると、AWS Fargate で実行されているコンテナを把握し、Amazon Fargate タスク (ECS) によって起動されたコンテナイメージに対して脆弱性とコンプライアンスのスキャンを実行し、結果を表示して修復アクションを実行できます。

AWS Fargate はサーバーレスであるため、このソリューションでは、新しい Fargate タスクがデプロイされるたびにセンサーが起動されます。AWS CloudFormation と Qualys Lambda 関数を使用して、スキャンを自動的にトリガーします。サブスクリプションの詳細を使用して CloudFormation テンプレートを設定し、Qualys S3 バケット名と S3 バケットキーを使用して Qualys Lambda 関数を設定し、Amazon Elastic Container Registry (ECR) からプルされたイメージのイメージスキャンをトリガーします。

仕組み

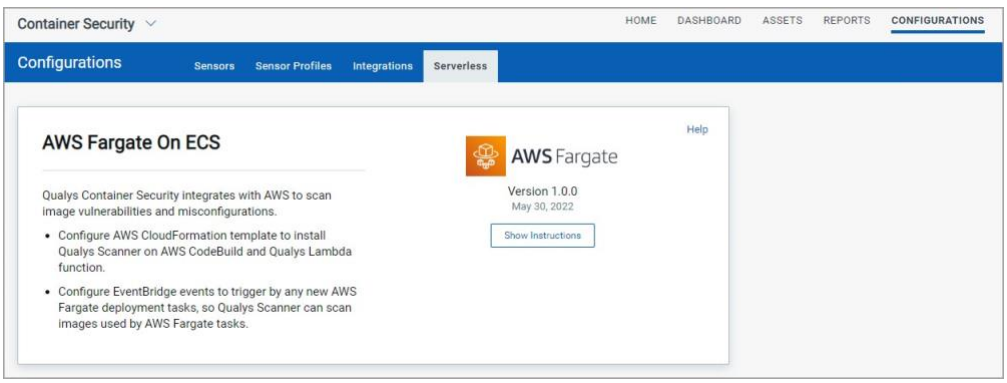
Amazon Elastic Container Registry からプルされた Docker イメージのスキャンをサポートしています。(Amazon ECR) を x86_64 アーキテクチャで使用します。AWS ECS Fargate タスクが起動されると、Qualys デプロイ中に作成された AWS EventBridge ルールがイベントを消費します。ザ

EventBridge ルールは、Qualys スキャン Lambda 関数をトリガーするように設定されます。その後、Qualys Lambda 関数は EventBridge から受信したイベントを処理して、イメージスキャンを決定します。Qualys Lambda 関数は、AWS CodeBuild を起動して Qualys センサーを実行し、Amazon ECR からイメージをプルし、イメージに対して脆弱性とコンプライアンスのスキャンを実行します。イメージ スキャンが成功すると、イメージ メタデータが評価のために Qualys Cloud Platform にアップロードされ、ユーザーは Container Security UI と API から詳細を表示できます。



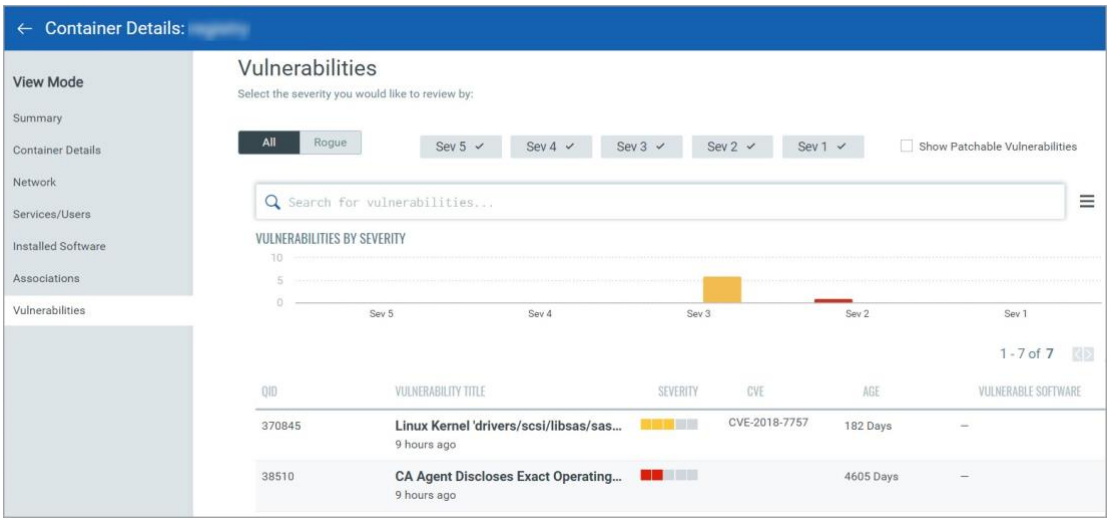
サーバーレス構成

Configuration の Serverless タブに移動します。[Show Instructions] ボタンをクリックして、設定手順の『Qualys Container Sensor Deployment Guide』を開きます。1 回限りの設定が完了すると、AWS Fargate の Amazon ECS タスクからデプロイされたすべてのイメージが自動的にスキャンされ、結果がアカウントにアップロードされます。



Docker コンテナの脆弱性スキャン

コンテナがスキャンされ、コンテナ内に脆弱性が存在するかどうかが確認されます。[Container Details] の [Vulnerabilities] パネルには、重大度が [脆弱性] とその QID のリストが表示されます。「Show Patchable Vulnerabilities」を選択して、使用可能なパッチがある脆弱性を表示します。



知っておくと良いこと

ドリフトコンテナは、コンテナの生成元のイメージにない脆弱性やソフトウェアを含むコンテナです。

不正な脆弱性 は、新規、修正済み、または変更済みのいずれかに分類されます。New は、コンテナで新しく見つかったが、コンテナの生成元のイメージには存在しなかったものです。修正済みは、コンテナではなくイメージで見つかった脆弱性です。コンテナとイメージの両方で検出される脆弱性はさまざまですが、検出はそれらによって異なります。

不正なソフトウェア は、新規または削除済みとして分類されます。新しいソフトウェアは、コンテナにはあるが、コンテナの生成元のイメージにはない。修正済み、ソフトウェアはコンテナに表示されませんが、親イメージには存在します。

Docker ホストの脆弱性スキャン

Container Security Sensor は、実際のホストマシンではなく、イメージとコンテナの脆弱性をスキャンします。ホストは、Scanner Appliance または Cloud Agent でスキャンできます。Cloud Agent を使用するためにホストで必要な設定は、センサーとは無関係です。たとえば、プロキシ構成などです。

レジストリのスキャン

Qualys Container Security を使用すると、パブリックレジストリとプライベートレジストリをスキャンできます。パブリックレジストリは、Amazon、Azure、Google でホストされているクラウドアクセス可能なレジストリです。一方、プライベートレジストリは、Artifactory や Nexus を使用してホストされているようなプライベートネットワーク上にデプロイされたオンプレミスレジストリです。Qualys は、認証されたレジストリーのみのスキャンをサポートします。注: 現在、Qualys Container Security では V2 タイプのレジストリのみをスキャンできます。次のレジストリのスキャンがサポートされています。

パブリックレジストリ: Docker Hub, AWS ECR, Google Cloud Registry (GCR), Google Artifact Registry, Azure Container Registry (ACR)

プライベートレジストリ:

- v2-private registry
- Docker Private Registry: insecure (http), secure (auth + https)
- Docker Trusted Registry
- Harbor
- JFrog Artifactory Private
- Mirantis Secure Registry (MSR) 2.9.4+
- OpenShift Container Registry (OCR)
- RedHat Quay
- Sonatype Nexus

注: http を使用するには、レジストリ用に docker-engine を手動で構成する必要があります。Qualys は http の使用を推奨しておらず、開発環境でのテストを目的としています。

各レジストリ タイプでサポートされるセンサー バージョンと、サードパーティ ソリューションとの相互運用性の詳細については、『Qualys Container Security Interoperability Matrix』を参照してください。

インストゥルメンテーションのサポートについては、「コンテナランタイムセキュリティ」を参照してください。

Docker ホストの要件

前提条件として、レジストリにアクセスしてスキャンするイメージをプルできる Docker ホスト (Docker、Containerd、または CRI-O ランタイムを使用) にレジストリ センサーをインストールする必要があります。

Docker バージョン: 1.12 以降

Docker ホストのディスク容量: Docker がインストールされているパーティションに 20 GB 以上の空き容量。これは、レジストリ イメージをスキャンするために必要です。さらに、永続ストレージには 1 GB の空き容量が必要です。

接続

レジストリ センサー ホストは、スキャンするレジストリに接続できる必要があります。ランタイムが Docker の場合は、ホストからレジストリへの Docker ログインを正常に実行することで、接続を検証できます。runtime が Containerd または CRI-O の場合は、レジストリから任意のイメージをプルして接続を検証できます。

Docker Runtime:

docker login <registryurl> (No protocol)

For Example:

docker login myregistry.com:5001

Containerd/CRI-O Runtime:

crictl pull anyimage from registry

レジストリスキャンはどのように機能しますか?

レジストリのスキャンは、リストフェーズとスキャン フェーズの 2 つのフェーズに分かれています。

リストフェーズ

リストフェーズでは、Container Security センサーが Docker Registry v2 API を呼び出して、レジストリ スキャン スケジュールで提供されるリポジトリのすべてのイメージ メタデータ情報を収集します。

Qualys センサーは、カタログ、タグ、マニフェスト、および構成の API 呼び出しを行って情報を収集し、この情報が UI に表示されます。ユーザーがスケジュールで定義したフィルター (過去 14 日間に作成されたスキャン イメージなど) に基づいて、イメージはスキャンのキューに入れられます。

注 - パブリック レジストリ(クラウドでアクセス可能)の場合、Qualys は Docker レジストリ API 呼び出しを行い、イメージ スキャンを実行するためのセンサーにフィードする情報を取得しま

す。プライベートレジストリの場合、Qualys はそれらに接続できないため、センサーはリストとスキャンの両方のアクションを実行し、Qualys に情報を送信します。

スキャニングフェーズ

レジストリ センサーとしてプロビジョニングされたセンサーは、定期的に Qualys をポーリングして、スキャン用にキューに入れられたイメージがあるかどうかを確認します。Qualys は、検出されたイメージのサブセットのみをスキャン用にセンサーに割り当てます。応答ペイロードには、イメージの詳細と、レジストリからイメージをプルするために必要な認証資格情報が含まれます。

Qualys レジストリ センサーは、レジストリからこれらのイメージを取得し、情報(スナップショット)を収集して Qualys クラウドにプッシュします。次に、Qualys は収集された情報に対してシグニチャを実行し、Container Security UI で表示できる脆弱性レポートを生成します。リポジトリにスキャンするイメージが多数ある場合、全体的なスキャン時間が通常よりも長くなる可能性があります。複数のレジストリ センサーをインストールしてスキャン ペイロードを分散し、スキャン時間を短縮し、結果をより高速に表示できます。

手順について

Container Security UI から、センサー イメージをダウンロードし、センサーがレジストリおよび Qualys と通信できるネットワーク内のレジストリ センサーとしてセンサーをデプロイします。次に、新しいレジストリを作成し、セキュリティ体制が必要なリポジトリでスキャンスケジュールを設定します。オンデマンド スキャンまたはスケジュール スキャンを実行できます。スケジュールされたスキャンは増分であるため、前回のスキャン以降に構成済みのリポジトリに追加された新しいイメージのみが考慮されます。

これらの手順について詳しく説明します。

Registry Sensor のインストール

スキャンする新しいレジストリーの追加

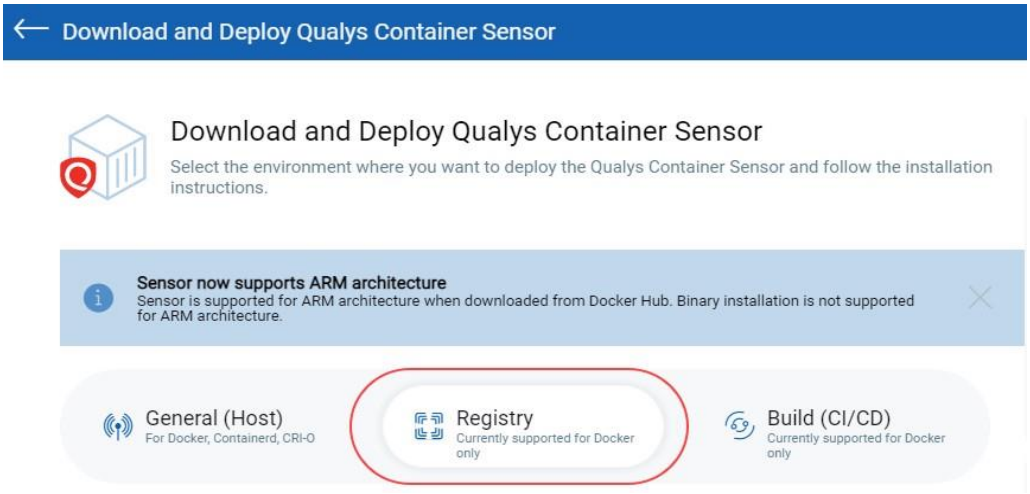
レジストリー・スキャン・スケジュールの作成

脆弱なレジストリー・イメージの表示

Registry Sensor のインストール

レジストリ センサーをダウンロードします。[Configurations > Sensors] に移動し、[Download Sensor] をクリックしてから [Registry] をクリックします。

レジストリ スキャン用のセンサーをインストールするには、センサー インストール コマンドに **--registrysensor** または **-r** を追加する必要があります。



スキャンする新しいレジストリーの追加

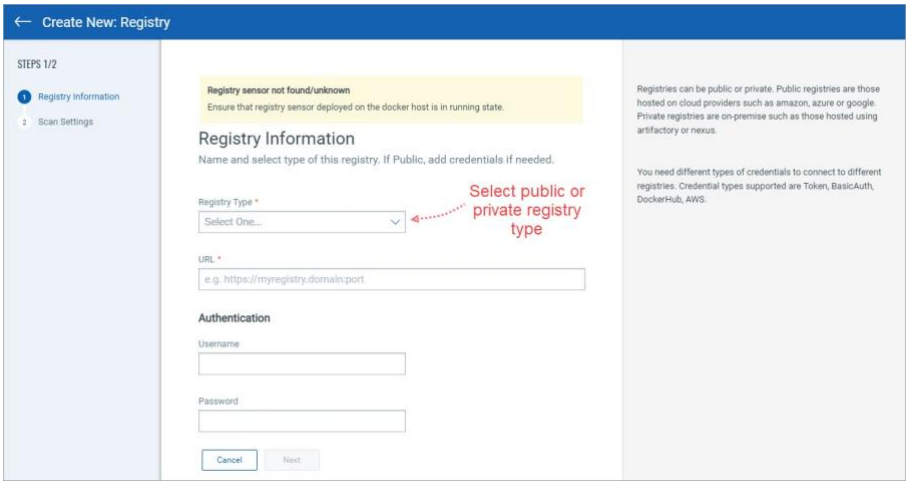
スキャンするには、レジストリを追加する必要があります。「Assets>Registries」に移動し、「New Registry」をクリックします 。

レジストリにて、Docker ホストにデプロイされたレジストリ センサーが Running 状態であることを確認します。

脆弱性とコンプライアンスの分析を実行するには、レジストリ認証を使用してレジストリに接続する必要があります。異なるタイプのレジストリーに接続するには、異なるタイプの認証が必要です。

レジストリ認証の種類は、Token、BasicAuth、DockerHub、AWS です。

注:トークン認証は、レジストリーがトークンベースの認証をサポートしている場合、レジストリーへの接続時にセンサー・ホストによって使用されます。



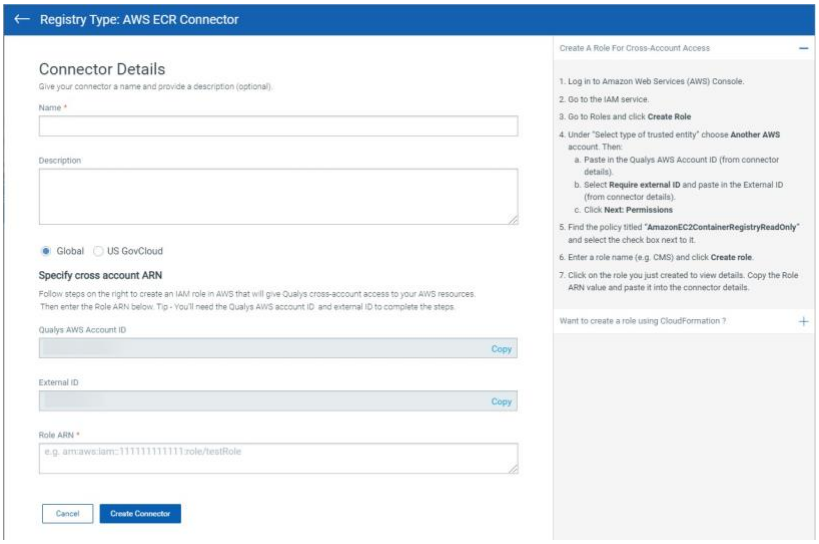
以下の表に、さまざまなプライベート・レジストリーの認証に必要な特権を示します。

Registry	Authentication Privileges Required	Description
JFrog Artifactory Private	Any user	Authenticate using either of the following: - Credentials of any user account - An access token
Mirantis Secure Registry (MSR) 2.9.4+	Administrator	Enter the credentials of an administrator account. Mirantis Secure Registry supports token-based authentication.
OpenShift Container Registry (OCR)	Registry-Viewer	Enter the service account credentials. The registry-viewer role must be associated with the service account.

RedHat Quay	Administrator or Super user	Enter the credentials for any of the following accounts: - An account with administrator or super user privileges - A robot account For the robot account, the username is formatted as UserName+RobotAccountName and the password is the password token value for the robot account.
Harbor Registry	Administrator	Enter the credentials of an administrator account. If your Harbor registry version supports token-based authentication, the sensor will perform the V2 catalog call with the authentication token. If authentication fails, the sensor will automatically fall back to the basic authentication method for the V2 catalog call.
Sonatype Nexus	Administrator	Enter the credentials of an administrator account.
Docker Trusted Registry	Any user	Enter the credentials of any user account.
Docker Private Registry: Secure and Insecure	Any user	Enter the credentials of any user account.

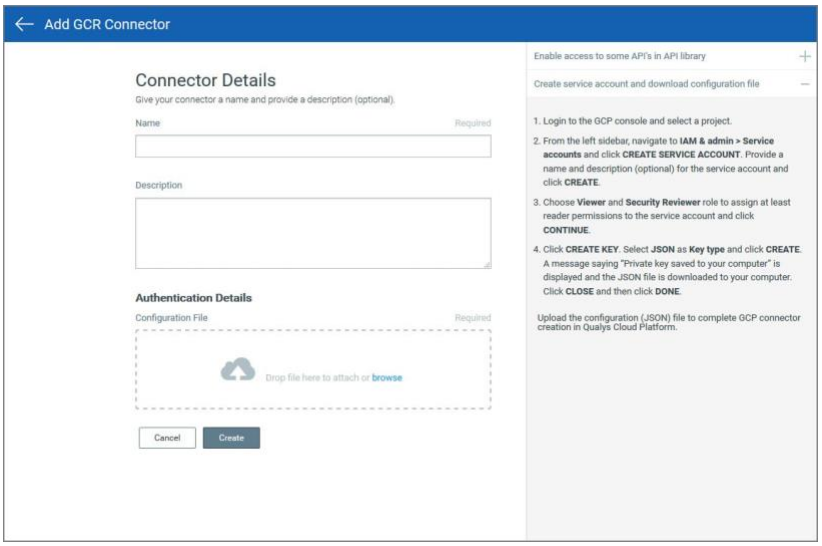
パブリック・レジストリーの場合、レジストリーに接続してリソースにアクセスするには、閲覧者特権を持つロールで十分です。

AWS ECR の場合、コネクタを作成して AWS Global または US GovCloud アカウントに接続できます。標準の AWS リージョンを選択した場合は、コネクタの詳細で [グローバル アカウントの種類] を選択します。US GovCloud リージョンを選択した場合は、コネクタの詳細で US GovCloud アカウントの種類を選択する必要があります。

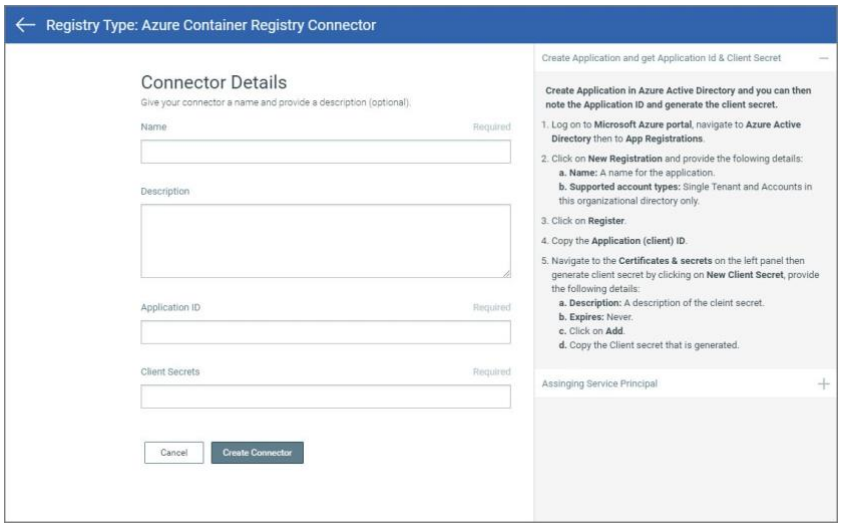


注: 現在、レジストリセンサーは AWS ECR プライベートリポジトリのみをスキャンできます。

GCR(Google Cloud Registry)の場合、GCP アカウントに接続するためのコネクタを作成できます。



ACR (Azure Container Registry) の場合は、Azure アカウントに接続するためのコネクタを作成します。



レジストリースキャン・スケジュールの作成

レジストリ情報を入力したら、手順 2 に進み、スキャン設定を指定します。

スキャンの種類

すぐにスキャン (オンデマンド)するか、継続的にスキャン(自動)するかを選択できます。オンデマンド スキャンでは、リポジトリ、それらのリポジトリ内の特定のイメージをスキャンできます (日付フィルターとタグ フィルターを使用します)。自動スキャンでは、ユーザー指定のスキャン スケジュールに従って、リポジトリ全体を定期的にスキャンできます。

リポジトリ

スキャンするリポジトリを 1 つ以上追加します。「リポジトリー」フィールドに、スキャンするイメージを含む最後のサブディレクトリーまでのフル・リポジトリー・パスを入力します。 ヒント: 次のコマンドは、レジストリーの一部であるフル・リポジトリー名のリストを取得するのに役立ちます。

```
curl -u <ユーザー名>:<パスワード> https://<レジストリ-url>/v2/_catalog
```

注意：

1. Google Cloud Registry の場合、レジストリ情報に場所をすでに指定しているため、リポジトリ名に位置情報を含めないでください。たとえば、リポジトリ名は project-Id/repository-name のようになります。
2. Google Artifact Registry の場合、リポジトリ名のみが必要です。完全なパスを自動入力します。

フィルターの使用 (オンデマンド スキャン用)

スキャンの種類が [オンデマンド] の場合、リポジトリ内の特定のイメージを選択してスキャンできるフィルターが表示されます。

日付別 – イメージが作成された日付に基づいてイメージのリストをフィルタリングします。［作成日］メニューで、イメージが作成されてから何日、何週間、または何か月前かのオプションのいずれかを選択します。

タグ別 – リポジトリ内でスキャンするイメージのリストをフィルタリングするには、それらのイメージに割り当てられたタグを選択します。タグ名を 1 つ入力し、［追加］をクリックします。次に、別のタグ名を入力して[追加]をクリックします。

JFrog Artifactory Private レジストリをお使いですか?この場合、タグ名で画像を選択する必要があります。画像がプッシュされた日付で画像をさらにフィルタリングできます。

プッシュ日 – このオプションを使用すると、各イメージがスキャン対象のリポジトリにプッシュされた日時に基づいて、スキャンするイメージをフィルタリングできます。「すべて」を選択すると、プッシュされた日付に関係なく、リポジトリにプッシュされたすべてのイメージがスキャンされ、指定した設定日数前にリポジトリにプッシュされたイメージのみがスキャンされます。

スキャン スケジュール (自動スキャンの場合)

自動レジストリ スキャン ジョブを実行する頻度 (毎日または毎週) を構成します。「スキャン・スケジュール」の「繰り返し」メニューからオプションを選択します。

日次スキャンの場合は、スキャンを開始する時刻を [開始時刻] メニューから選択します。スキャンは、毎日選択した時刻に開始されます。

週単位のスキャンの場合は、曜日と開始時刻を選択します。スキャンは、毎週、指定された日時に行われます。

すべてのイメージをスキャンする: [Scan All images]オプションを選択すると、レジストリ スキャンが開始されるたびにレジストリ内のすべてのイメージをスキャンできます。サブスクリプションでこの機能を有効にする必要があります。テクニカル アカウント マネージャーまたは Qualys サポートに問い合わせて有効にしてください。

スキャンをキャンセルする方法

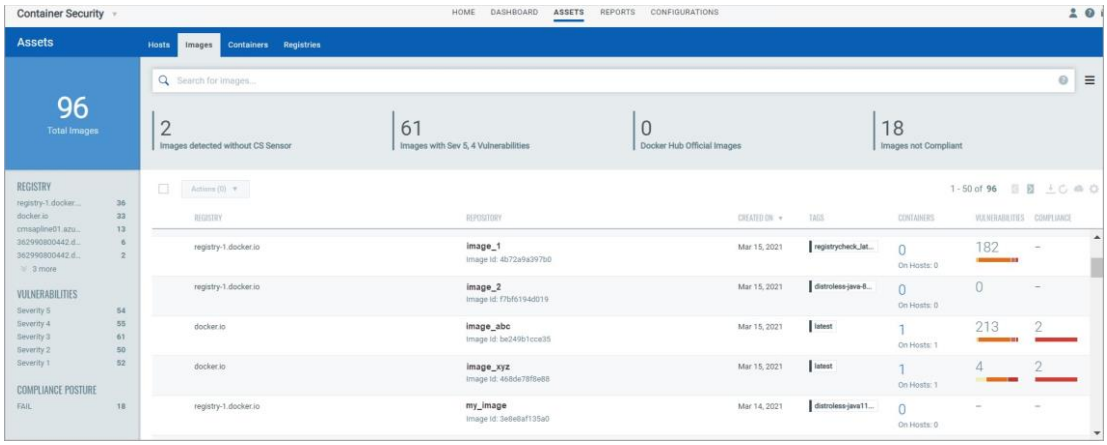
進行中のスキャンを取り消すには、レジストリを編集し、スキャン ジョブの [クイック アクション] メニューの [キャンセル] オプションを使用します。「エラー」または「完了」状態のジョブはキャンセルできません。

スキャンを再開する方法

[**再スキャン**] オプションを使用して、オンデマンド スキャンを再開します。「キュー」または「実行中」状態のスキャン ジョブを再開することはできません。

脆弱なレジストリイメージの表示

レジストリに接続すると、Container Security はインベントリ データをプルし、レジストリ内のリポジトリとイメージに対してスキャンを実行します。画像は「**アセット**」>「**画像**」タブに一覧表示されます。



レジストリ内の脆弱なイメージの合計数を取得するには、[アセット] > [レジストリ] タブに移動し、任意のレジストリの [クイック アクション] メニューから [詳細の表示] を選択します 。リポジトリの合計数、イメージの合計数、脆弱なイメージの合計数などの基本情報が表示されます。また、レジストリをスキャンするために作成されたスキャン スケジュールの一覧も表示されます。

脆弱性の例外の定義 (ベータ)

必要な脆弱性に、特定のイメージとコンテナの例外としてフラグを立てることができます。

脆弱性の例外とは、コンテナー化された環境内で特定されたが、修復措置から意図的に除外されている特定の脆弱性を指します。

例外を認める理由として考えられるのは、次のような場合です。

1. **誤検知**: 報告された脆弱性の一部は誤検知である可能性があります。
2. **サードパーティ**の依存関係: サードパーティのライブラリまたはコンポーネントには、直接制御できない特定の脆弱性が存在する可能性があります。
3. **互換性の問題:** 脆弱性の修正プログラムを適用すると、他の影響が生じる可能性があります。

脆弱性の例外を定義するには、「例外」**>「脆弱性の例外」を参照してください**。

詳細については、オンラインヘルプ:脆弱性の例外の定義を参照してください。

セキュリティポリシーの定義

コンテナ化された環境で設定、脆弱性管理、コンプライアンス、アクセス、監査を管理するためのポリシーを Container Security で作成できるため、イメージとコンテナを保護するプロセスを自動化できます。ポリシーは、イメージやコンテナーなどの特定の成果物を評価するルールの組み合わせを提供し、ルールに関連付けられたアクションを提供します。

現在、CICD の画像評価ポリシーのみを使用できます。デプロイ前に既知の脆弱性のコンテナイメージをスキャンするためのルールを定義し、CICD ビルドのブロックやアラートのトリガーなど、特定の重大度の脆弱性の数を超えた場合に実行するアクションを指定できます。

[**ポリシー**] タブに移動して、新しいポリシーを作成します。詳細については、オンラインヘルプ: セキュリティポリシーの作成を参照してください。

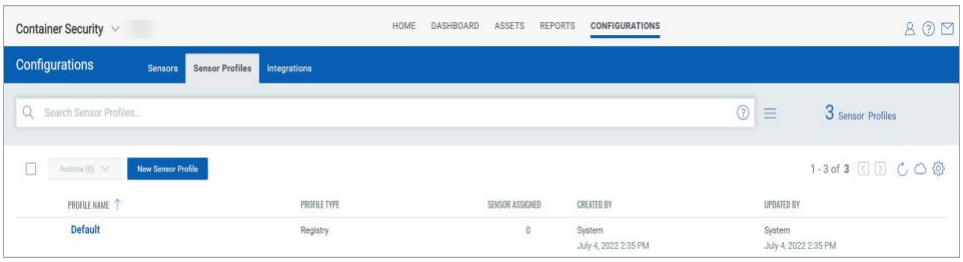
センサープロファイル

センサー プロファイルを作成し、設定値を編集し、プロファイルをセンサーに割り当てることができます。

レジストリ センサーの場合、センサー プロファイルを構成して、さまざまなレジストリのスキャンに使用するセンサーを制御することができます。各プロファイルは、レジストリのリストと、それらをスキャンできるセンサーのリストを関連付けます。これは、インターネットにアクセスできず、クラウドベースのレジストリをスキャンできないセンサーがある場合に特に便利です。これで、クラウドベースのレジストリでプロファイルを作成し、スキャンのためにそれらに到達できるセンサーのみを含めることができます。

知っておくと良いこと

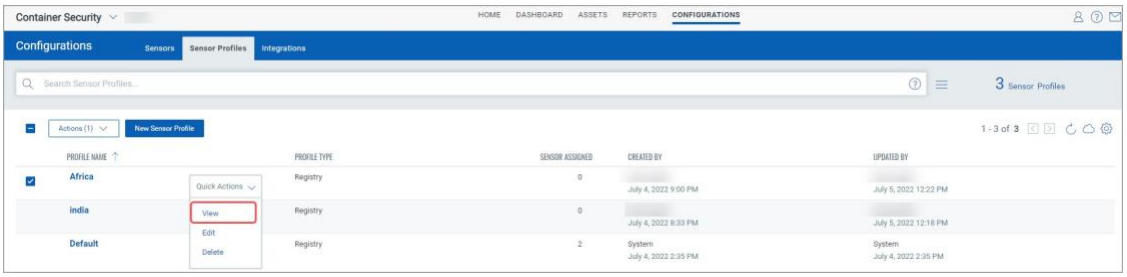
1. センサー プロファイルをセンサーに関連付けない場合は、デフォルトのセンサー プロファイルが使用されます。
2. 1 つのセンサーを 1 つのセンサー プロファイルにのみ関連付けることができます。
3. レジストリセンサーの場合、センサー プロファイルに複数のレジストリを追加できます。
4. スキャン時には、レジストリに関連付けられているセンサーのみがスキャン ジョブに使用されます。レジストリがセンサー プロファイルに含まれていない場合は、任意のセンサーを使用してスキャンできます。
5. 既定では、どのプロファイルにも関連付けられていないすべてのセンサーとレジストリは、既定のセンサー プロファイルの下に表示されます 。デフォルト・プロファイルのレジストリーは、デフォルト・センサー・プロファイルで使用可能な任意のセンサーからスキャンできます 。



センサープロファイルの表示

センサー プロファイルは、[構成] の [**センサー プロファイル**] タブに一覧表示されます。検索フィールドでは、プロファイル名、プロファイル UUID、プロファイルを作成または更新したユーザーの名前など、さまざまな条件でセンサー プロファイルを検索できます。

リスト内のプロファイルの詳細を表示するには、[**クイックアクション**] メニューから [表示] を選択します。



センサー プロファイルの追加、センサー プロファイルの更新、センサー プロファイルの削除などのアクションを実行するには、**オンライン ヘルプ**の「センサー プロファイルの管理」セクションを参照してください。

脆弱性の報告

カスタマイズ可能な QQL クエリ駆動型のオンデマンド レポート ジョブを作成します。レポートは、レポートテンプレートによって駆動されます。現在、イメージとコンテナの脆弱性レポートテンプレートをサポートしています。レポートワークフローは、Container Security UI の「レポート」タブから実行できます。

次の脆弱性レポートテンプレートを使用できます。

1. イメージ脆弱性レポート
2. コンテナ脆弱性レポート

イメージ脆弱性レポート

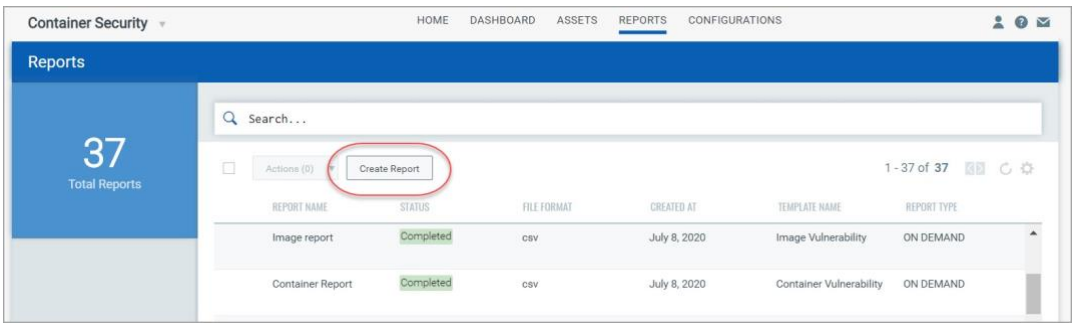
レポートの各行には、検出された 1 つの脆弱性のイメージの詳細 (リポジトリ、イメージ ID、SHA など) が表示され、その後に脆弱性の詳細 (QID、タイトル、重大度など) が表示されます。イメージに複数の脆弱性がある場合は、複数回一覧表示されます (たとえば、同じイメージの 10 個の脆弱性に対して 10 行)。

コンテナ脆弱性レポート

レポートの各行には、コンテナの詳細(コンテナ名、コンテナ ID、ホスト名など)が表示され、その後に、検出された 1 つの脆弱性の脆弱性の詳細(QID、タイトル、重大度など)が表示されます。コンテナに複数の脆弱性がある場合は、複数回一覧表示されます(たとえば、同じコンテナ上の 10 個の脆弱性に対して 10 行)。

レポートの作成

トップメニューの[レポート]セクションに移動し、[レポートの作成]ボタンをクリックします。



[新しいレポートの作成] **ウィザードの手順を実行します。[レポートの詳細]** セクションで、レポートの名前と説明を入力します。**[レポートソース(Report Source)]** セクションで、作成するレポ

ートのタイプ([イメージの脆弱性(Image Vulnerability)] または [コンテナの脆弱性(Container Vulnerability)])のレポートテンプレートを選択します。

検索クエリを追加して、レポートを特定の画像/コンテナーに制限することもできます。画像の脆弱性レポートでは、クエリに一致する画像のみが含まれます。コンテナーの脆弱性レポートでは、クエリに一致するコンテナーのみが含まれます。

「レポート・スケジュール」セクションで、オンデマンド・レポートを作成するか、**スケジュール・レポート**を作成するかを指定します。スケジュールされたレポートの場合は、レポートを定期的に実行するスケジュールを定義する必要があります。日次、週次、または月次の定期的なスケジュールを作成できます。

「**レポート表示**」セクションには、レポートに含めることができる詳細のタイプが表示されます。レポートに含める各詳細の横にあるチェックボックスを選択するだけです。選択内容によって、CSV 出力に表示される列が決まります。特定の詳細がデフォルトで選択されており、チェックを外すことができないことに注意してください。すべての詳細を含めたいですか?「すべて選択」オプションを選択すると、すべての詳細が含まれます。

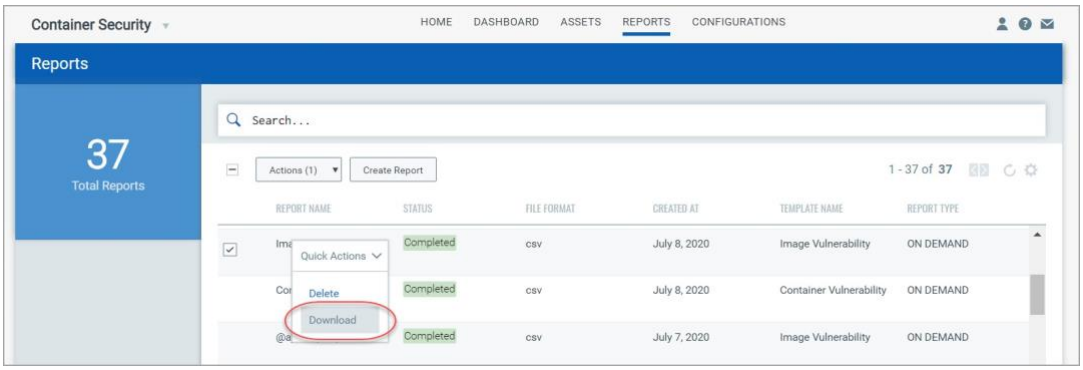
オンデマンド レポートの場合は、レポートの日付と時刻を表示するタイム ゾーンを指定します。

もう一度「次へ」をクリックして「**レポート・サマリー**」を確認し、「**送信**」をクリックしてレポート・ジョブを生成します。いったん保存すると、レポートジョブは編集できません。

レポート ジョブは、レポート リストに Accepted のステータスで表示されます。ステータスはレポートが完了し、ダウンロードの準備が整うと Completed に変わります。

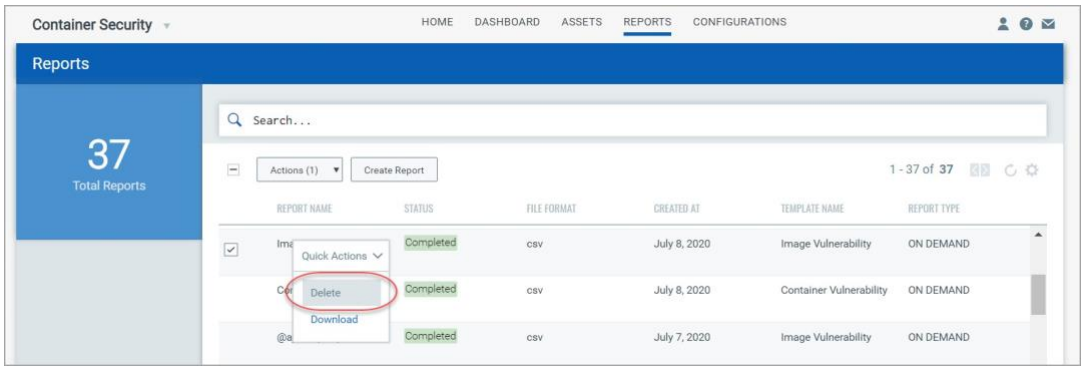
レポートの表示とダウンロード

完成したレポートの [クイック アクション] メニューから [ダウンロード] を選択します。CSV レポートは、ローカルのダウンロードエリアに保存されます。(ヒント - レポート リストの上にある [検索] フィールドを使用すると、検索トークン reportName を使用してレポートをすばやく検索できます。



レポートの削除

1 つのレポートを削除するには、 次に示すように、[クイックアクション] メニューから [削除] を選択します。複数のレポートを一括で削除するには、削除するレポートの各行を選択し、レポート リストの上にある [アクション] > [削除] を選択します。



コンプライアンス スキャン

Qualys は、実行中のコンテナとイメージのコンプライアンススキャン/評価をサポートしています。実行中のコンテナーとイメージに対してポリシー コンプライアンス (PC) チェックと構成評価を実行します。CIS Docker ベンチマークのコントロールのサブセットがサポートされており、実行中のコンテナーとコンテナー イメージに適用できます。お客様は、実行中のコンテナとイメージの構成リスクを評価し、Qualys の調査結果に基づいて適切に修正できます。

前提 条件

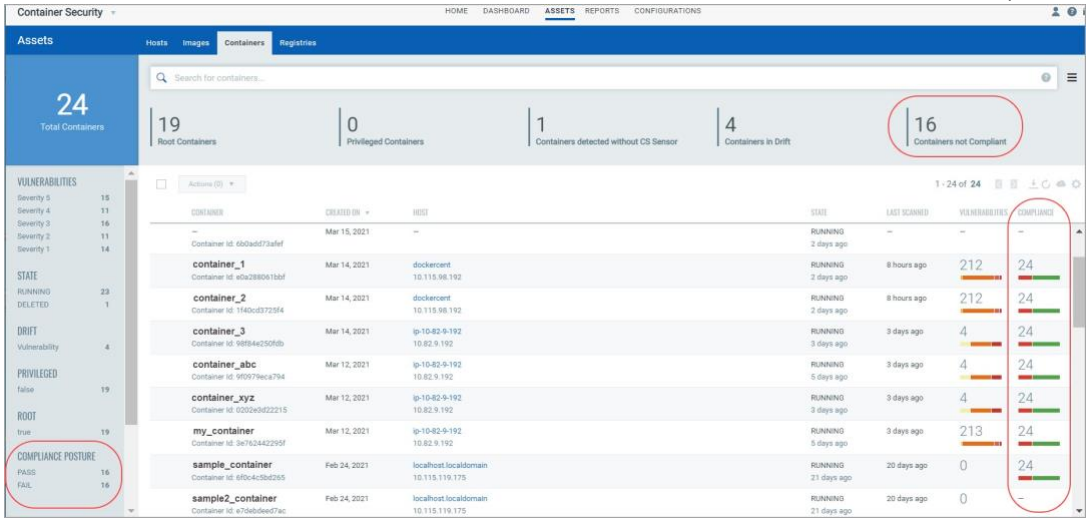
センサーを最新バージョン (センサー バージョン 1.9.0 以降) にアップグレードします。

仕組み

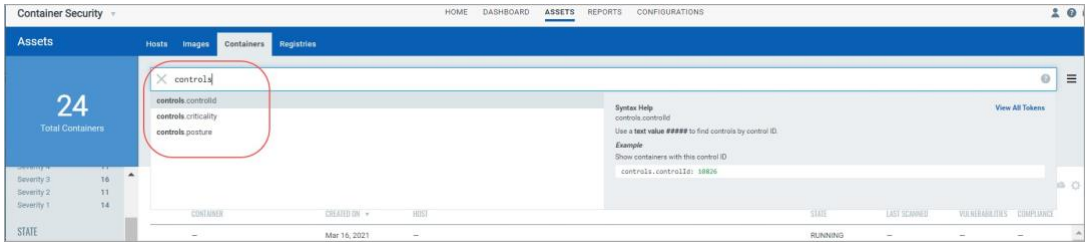
更新された Qualys コンテナ センサーは、コンテナ、イメージ内の設定の追加スキャンを実行し、追加のスキャン メタデータを Qualys バックエンドにアップロードします。バックエンドは、スキャンメタデータに基づいて、コンプライアンス評価のためのさまざまな業界標準のベンチマークとコントロールに対する評価を実行します。コンテナやイメージのコンプライアンススキャンは、お客様に対して透過的であり、脆弱性スキャン機能と同様にリアルタイムのクラウドネイティブな方法で機能します。構成スキャンの結果は、UI と API で使用できます。UI で、イメージとコンテナーの詳細を表示して、コンプライアンス体制 (PASS または FAIL) と制御情報を取得します。

コンプライアンス情報の表示

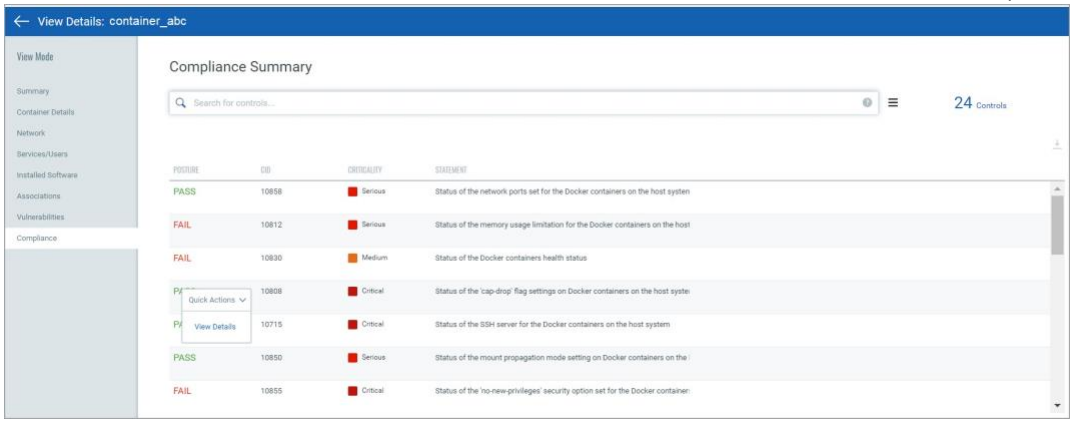
イメージとコンテナーの UI にコンプライアンス情報が表示されます。[イメージ] リストと [コンテナー] リストに、[コンプライアンス] という列が表示され、状態が PASS と FAIL のコントロールの数が表示されます。コンテナーのサンプル リストを次に示します。



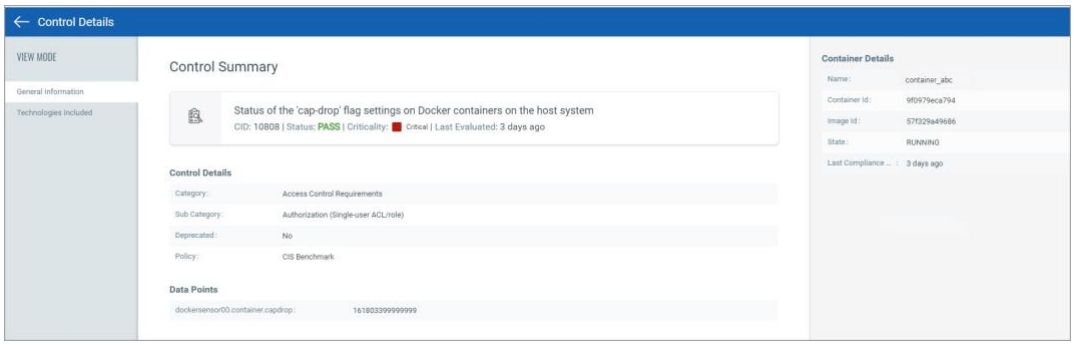
コントロール ID、コントロールの重要度(MINIMAL、MEDIUM、SERIOUS、CRITICAL、URGENT)、コントロールポスチャ(PASS、FAIL)でイメージとコンテナを簡単に検索できます。



イメージまたはコンテナーの詳細にドリルダウンして、コントロールの詳細 (CID、重要度、ステートメント、カテゴリ、テクノロジ) でスキャンされたコントロールの一覧など、コンプライアンス情報を表示します。



任意のコントロールの詳細にドリルダウンして、コントロールのカテゴリ、ポリシー、テクノロジなど、コントロールの詳細を取得します。



コンプライアンス情報は、コンプライアンス API を使用して取得することもできます。イメージまたはコンテナーのコンプライアンス体制をフェッチしたり、コントロールの詳細をフェッチしたり、コントロールのリストをフェッチしたりできます。『Qualys Container Security API ガイド』の「コンプライアンス」セクションを参照してください。

SCA スキャン

Qualys は、コンテナイメージのソフトウェアコンポジション分析 (SCA) スキャンをサポートしています。SCA スキャンは、コンテナイメージに存在する、インストールされているオープンソースソフトウェアとライブラリ、および関連する脆弱性を検出します。

コンテナイメージのセキュリティ体制を評価する際には、イメージに存在するすべてのソフトウェアパッケージを特定することが重要です。SCA スキャンは、イメージ内のプログラミング言語ベースのソフトウェア・パッケージを識別するために使用できます。さらに、各画像レイヤーのメタデータ情報も提供されます。SCA スキャンは、Java、Python、Go、Node.js、.NET、PHP、Ruby、および Rust のプログラミング言語のパッケージを検出します。

SCA スキャンは、すべてのセンサーの種類 (一般、レジストリ、CI/CD) で使用でき、Docker、containerd、および CRI-O ランタイムでサポートされています。また、SCA スキャンは、コンテナー・イメージをスキャンする場合にのみサポートされます。SCA スキャンは Mac OS ではサポートされていません。

前提 条件

1. サブスクリプションで SCA スキャン機能が有効になっている必要があります。Qualys サポートに連絡して、この機能を有効にしてください。
2. センサーをセンサー バージョン 1.19 以降に更新します。
3. パラメーター --perform-sca-scan **を使用してセンサーを再起動し** 、SCA スキャンを実行します。

仕組み

SCA スキャンは、デフォルトでは実行されません。ユーザーは、センサーをデプロイするときに、新しいパラメーター --**perform-sca-scan** を使用して SCA スキャンを有効にする必要があります。有効にすると、コンテナイメージの標準脆弱性スキャン(静的または動的)の後に SCA スキャンが実行されます。SCA スキャンが完了すると、センサーはスキャンによって収集されたメタデータ情報を、ポスチャ評価が実行される Qualys バックエンドにアップロードします。SCA スキャン・データの検出結果は、イメージの詳細の一部として、Container Security UI および API で表示できます。SCA スキャンによって検出された脆弱性検出は、QID として表示されます。特定の脆弱性の検出に使用されるスキャンのタイプ (SCA、動的、または静的) を識別できるように、フィルターが用意されています。

SCA スキャンでは、言語固有のソフトウェア・パッケージについて以下のファイルがスキャンされます。

言語	ファイル
Python	egg package wheel package
Node.js	package.json
Java	JAR/WAR/PAR/EAR
Go	Binaries built by Go
PHP	Composer.lock
Ruby	gemspec
Rust	Cargo.lock and Binaries built with cargo-auditable

SCA スキャン・イメージの表示

画像を検索するには、[**Asset** > **Image**] に移動します。**scanType** を使用して、イメージのスキャンに実行されたスキャンのタイプ (動的、静的、または SCA) に基づいてイメージを検索します。

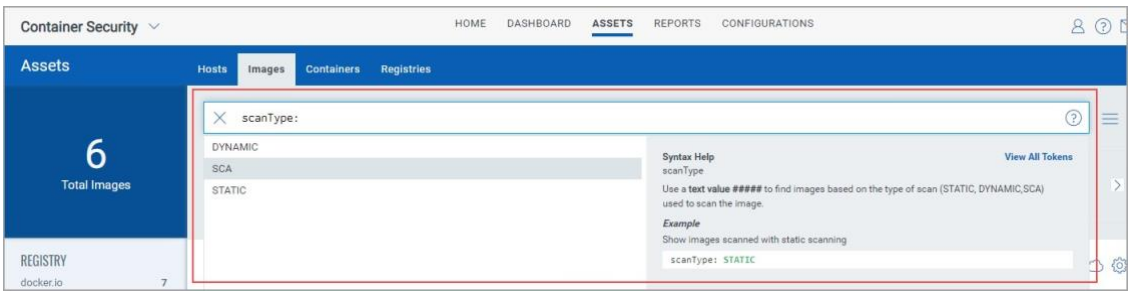
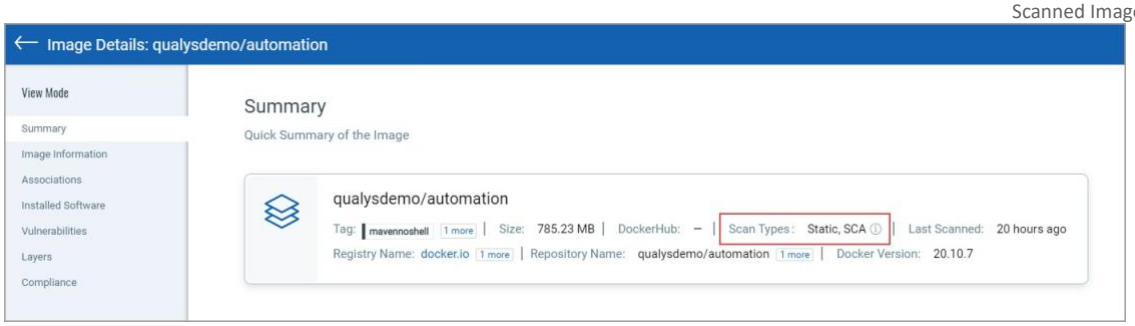


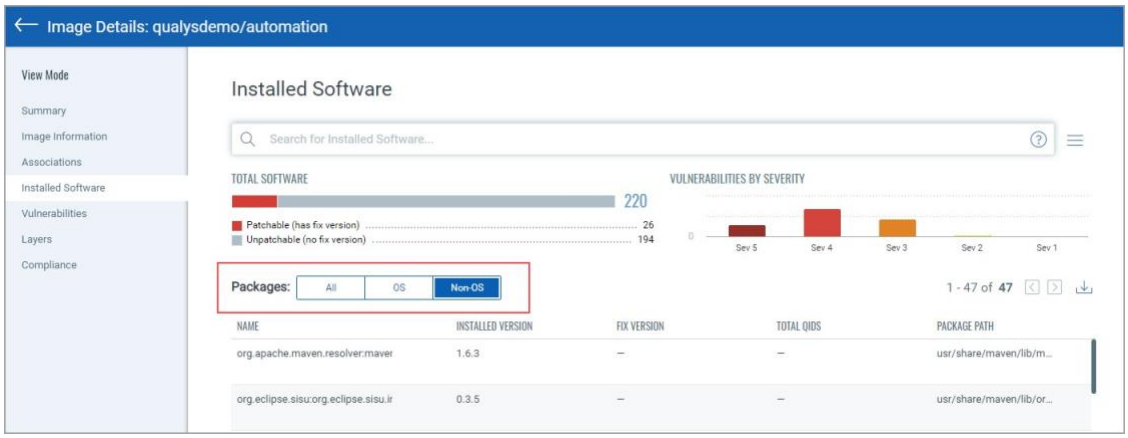
Image の詳細を表示

[Assets > Images] に移動し 、リストされているイメージの [View Details (詳細の表示)] を選択します。

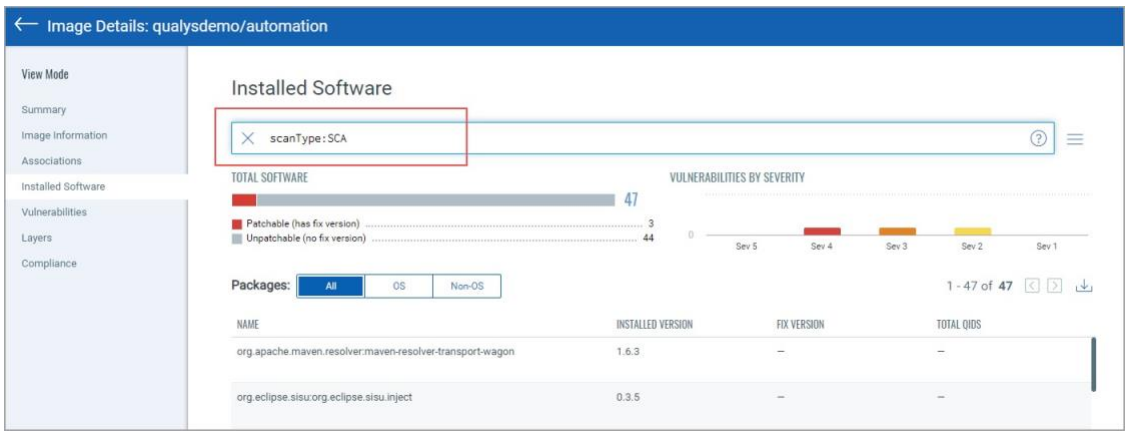
[**概要**] タブには、イメージに関する一般的な情報が表示されます。「**スキャン・タイプ**」フィールドには、SCA を含む、イメージに対して実行されたスキャンのタイプが表示されます。



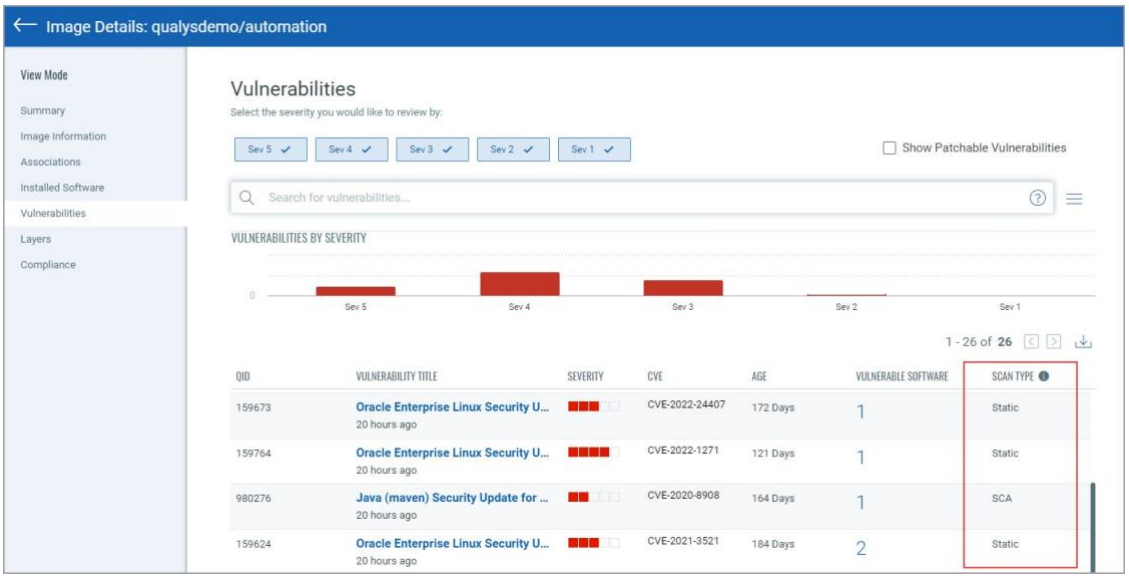
「**インストール済みソフトウェア**」タブには、スキャンで検出されたソフトウェアがリストされます。[パッケージ] フィルターを使用すると、リストビューを簡単に切り替えることができます。 **すべてのソフトウェアパッケージを表示するには [**すべて] を選択し、オペレーティングシステムベースのパッケージのみを表示するには **[OS]** を選択し、SCA 関連パッケージを表示するには **[**非 OS] を選択します。



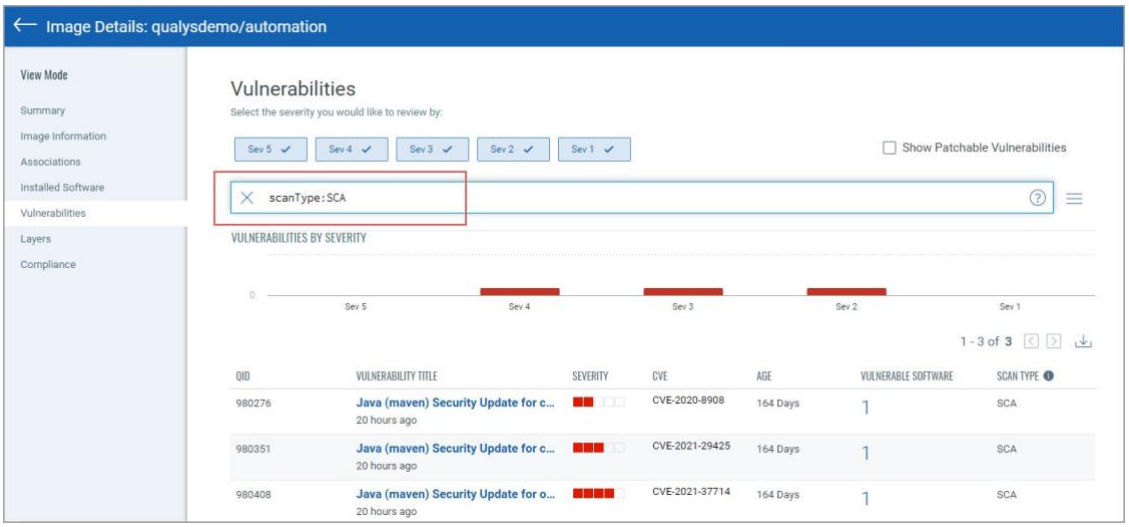
scanType: SCA を使用して、SCA スキャンによって検出されたインストール済みソフトウェアを検索することもできます。



「**脆弱性**」タブには、SCA スキャンを含むすべてのスキャンで検出された脆弱性が表示されます。「スキャン・タイプ」列は、各検出に使用されるスキャンのタイプを識別します。



scanType: SCA を使用して、SCA スキャンで検出された脆弱性を検索することもできます。



脆弱性数に関する注意

SCA によってスキャンされたイメージについて報告された脆弱性の数と、イメージから起動されたコンテナーの脆弱性の数に違いがあることに気付くでしょう。これは、SCA スキャンがイメージでのみ実行され、コンテナーでは実行されず、SCA スキャンがパッケージベースの脆弱性を検出するためです。つまり、イメージスキャンは OS ベースの脆弱性、OS または SCA パッケージ以

外の脆弱性を含むすべての脆弱性を報告しますが、コンテナスキャンは OS ベースの脆弱性のみを報告します。

たとえば、Perform SCA フラグを有効にして起動したセンサーを使用してイメージをスキャンしたところ、25 件の脆弱性が報告されたとします。このイメージでコンテナを起動すると、22 件の脆弱性が報告されています。3 件の脆弱性はパッケージベースであるため除外されました。

シークレット検出

コンテナシークレットは、ID 認証を提供し、特権アカウント、アプリケーション、サービスへのアクセスを承認するデジタル認証情報です。これには、アプリケーションが正しく機能するために必要なパスワード、API キー、およびその他の資格情報を含めることができます。

これらのシークレットが適切に保護されていないと、権限のないユーザーがアクセスし、悪意のある攻撃につながる可能性があります。したがって、シークレットの検出は、機密データを保護し、コンプライアンス要件を満たし、セキュリティインシデントのリスクを軽減するために組織が優先する必要があるコンテナセキュリティの重要な側面の 1 つです。

Container Security は、コンテナイメージのシークレットを検出できるため、コンテナ内のシークレットの偶発的または意図的な公開に関連する潜在的なセキュリティリスクを軽減できます。

[**Configuration > Secret Detection**] タブでは、シークレットディテクタまたはさまざまなタイプのシークレットを識別するための一連のルールを確認できます。現在、デフォルトのシステム定義ディテクタのみを使用できます。

「クイック・アクション」メニューから「詳細の表示」**をクリックして**、ディテクタの詳細を表示します。現在、新しいディテクタを作成したり、既存のディテクタを変更したりすることはできません。

注: シークレット検出は、以下でのみサポートされます。

- Sensors: CICD and registry

- OS: Linux

- Runtimes: Docker, Containerd, and CRI-O

詳細については、オンラインヘルプ Detecting Container Secrets.を参照してください。

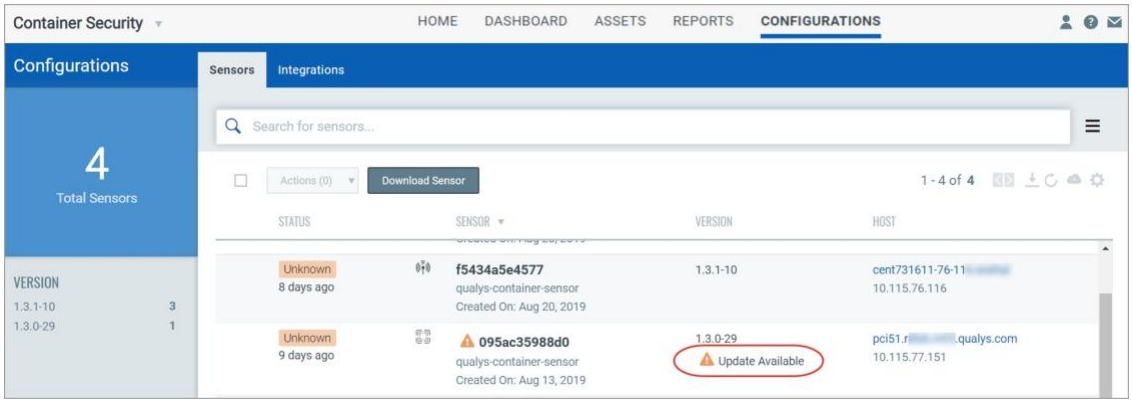
Administration

センサーの設置とトラブルシューティングについては、 Qualys Container Security Sensor Deployment Guide. をご参照下さい。

センサーの更新

[Configurations > Sensors] に移動して、センサーのリストを表示します。検索オプションとフィルター オプションを使用して、センサーを検索します。QQL 検索トークンのリストについては 、オンライン・ヘルプを参照してください。

デプロイされたものよりも新しいセンサー バージョンが使用可能な場合は、センサー名の横に [利用可能な更新プログラム] と表示されます。センサーを新しいバージョンに更新して、新機能やバグ修正を活用し、脆弱性を修正する必要があります。



Qualys UI からダウンロードしたセンサーの場合

installsensor.sh script または docker run コマンドを使用して Docker にデプロイされたセンサーは、自動的に更新されます (インストール スクリプトに --disable-auto-update オプションが使用されていない場合)。センサーは、Kubernetes デプロイ用に自動的に更新されません。手順について

は、『Qualys Container Security Sensor Deployment Guide』の「Update the sensor deployed in Kubernetes」を参照してください。

Docker Hub からインストールされたセンサーの場合

Docker Hub でホストされている Qualys Container Sensor イメージは、自動更新をサポートしていません。手順については、『Qualys Container Security Sensor Deployment Guide 』の「Installing the sensor from Docker Hub」セクションの「Upgrading the sensor」を参照してください。

センサーのアンインストール方法

QualysContainerSensor.tar.xz ファイル(Qualys Cloud Platform からセンサーをインストールするためにダウンロード)には、センサーを**アンインストールするためのスクリプト** uninstallsensor.sh が含まれています。

センサーをアンインストールするには:

Docker ホストが docker.sock 経由で通信するように構成されている場合は、次のコマンドを使用します。

```
./uninstallsensor.sh -s
```

Docker ホストが TCP ソケットを介して通信するように構成されている場合は、Docker デーモンがリッスンするように構成されているアドレスを指定します。

```
./uninstallsensor.sh DockerHost=<<IPv4 address or FQDN>:<Port#>> -s
```

例 :

```
./uninstallsensor.sh DockerHost=10.11.12.13:1234 -s
```

画面の指示に従って、センサーをアンインストールします。Qualys では、永続ストレージをクリアしないことを推奨しています。