



Virtual Scanner Appliance

ユーザガイド

2019年8月27日

無断複写・転載を禁じます。2012-2019 年 クオ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。

クオリスジャパン株式会社

〒 100-6208

東京都千代田区丸の内 1-11-1

パシフィックセンチュリープレイス 8 階

03-6860-8296



目次

| | |
|--|-----------|
| 本書について | 4 |
| Qualys について | 4 |
| Qualys サポート | 4 |
| 操作手順 | 5 |
| 簡単に追加できる Virtual Scanner | 5 |
| Virtual Scanner の追加 | 6 |
| 役立つその他の機能 | 11 |
| 設定 | 12 |
| トラブルシューティング | 16 |
| アクティブ化コードが表示される理由 | 16 |
| Communication Failure メッセージ | 16 |
| アプライアンス設定エラー | 17 |
| スキャナに返された IP が不正で接続または表示に問題がある場合 | 18 |

本書について

Qualys Virtual Scanner Appliance は、Qualys の物理アプライアンスと同じグローバルスキャン機能を提供します。Virtual Scanner Appliance は、Qualys クラウドプラットフォームの拡張機能として自由に使用できるステートレスなリソースであり、個別に管理する製品ではありません。このユーザガイドでは、仮想化またはクラウドプラットフォームで Virtual Scanner の使用を開始する方法について説明します。

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。詳細情報は、www.qualys.com をご覧ください。

Qualys サポート

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

操作手順

簡単に追加できる Virtual Scanner

アカウントへの Virtual Scanner の追加は、数分で完了します。追加が完了すると、内部ネットワークでデバイスと Web アプリケーションをスキャンできるようになります。

サポートされる仮想化プラットフォーム



Qualys Virtual Scanner Appliance は、さまざまな仮想化プラットフォームやクラウドプラットフォームに導入できるようパッケージ化されたアプライアンスです。

デスクトップ/ノートパソコン

VMware Workstation、Player、Workstation Player、Fusion

クライアント/サーバ

VMware vSphere: vCenter Server、ESXi

Citrix XenServer

Microsoft Windows Server (Microsoft Hyper-V)

クラウド

Amazon EC2-Classical

Amazon EC2-VPC

Microsoft Azure Cloud Platform (ARM)

Google Cloud Platform

OpenStack

OCI および OCI-Classical

Alibaba Cloud Compute

適切なプラットフォームの選択

Qualys コミュニティには、サポートされている仮想化プラットフォーム、設定、使用可能なディストリビューションなど、適切なプラットフォームを選択するためのあらゆる詳細情報があります。

Qualys コミュニティより (英語)

[Virtual Scanner Appliance - Platform Qualification Matrix](#)

[Reference - Virtual Scanner Appliance](#)

インスタンス管理について

インスタンススナップショット/クローンはできません

Virtual Scanner インスタンスのスナップショットまたはクローンを使用して新規インスタンスを作成することは禁止されています。新規インスタンスはスキャナとして機能しません。すべての設定およびプラットフォーム登録情報は失われます。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

登録したスキャナインスタンスを、仮想化プラットフォーム（HyperV、VMware、XenServer）からクラウドプラットフォーム（AWS、Azure、GCE、OpenStack）に移動またはエクスポートすることは、いずれのファイル形式であっても厳格に禁止されています。これによりスキャナ機能が破損し、スキャナの設定は永久的に失われます。

必要事項

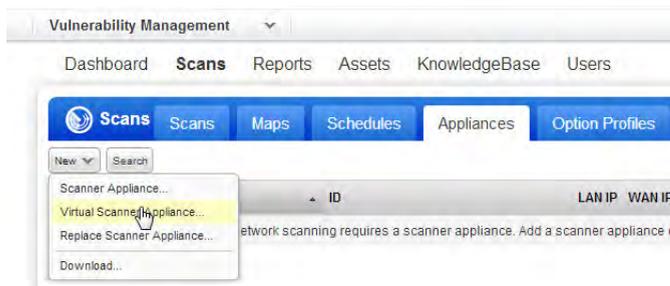
アカウントで「Virtual Scanner」オプションが有効になっている必要があります。このオプションを有効にするには、Qualys のサポートまたはテクニカルアカウントマネージャにお問い合わせください。

「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。

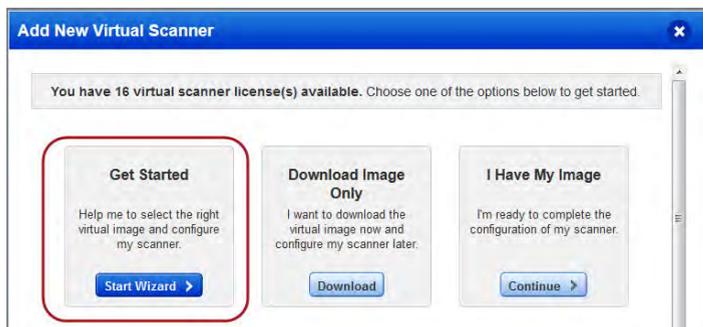
Virtual Scanner の追加

ステップ1 - ウィザードの開始

「Scans」→「Appliances」に進み、「New」→「Virtual Scanner Appliance」を選択します。

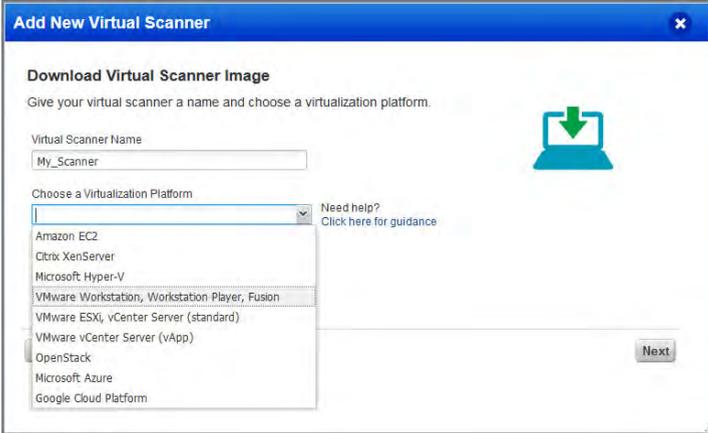


「Start Wizard」をクリックして、ウィザードのステップを開始します。



ステップ 2 - 仮想化プラットフォームの選択

スキャナの名前を入力し、使用する仮想化プラットフォームを指定します。



Add New Virtual Scanner

Download Virtual Scanner Image

Give your virtual scanner a name and choose a virtualization platform.

Virtual Scanner Name
My_Scanner

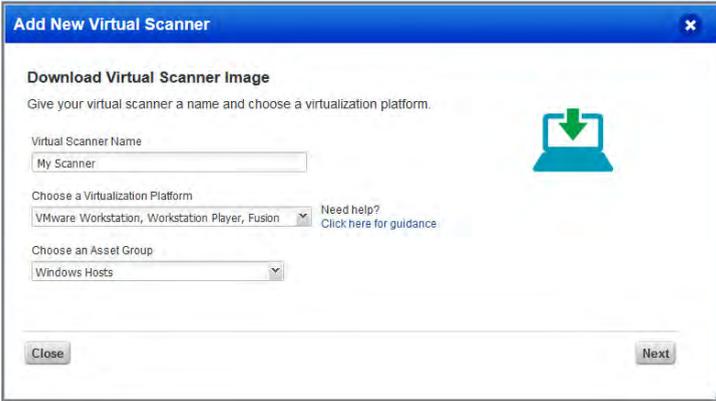
Choose a Virtualization Platform

- Amazon EC2
- Citrix XenServer
- Microsoft Hyper-V
- VMware Workstation, Workstation Player, Fusion
- VMware ESXi, vCenter Server (standard)
- VMware vCenter Server (VApp)
- OpenStack
- Microsoft Azure
- Google Cloud Platform

Need help?
Click here for guidance

Next

サブユーザの場合、マネージャユーザによってビジネスユニットに割り当てられたアセットグループを選択する必要があります。アセットグループがない場合アセットグループ（すべてのグループを除く）をビジネスユニットに割り当てるよう、マネージャに依頼してください。



Add New Virtual Scanner

Download Virtual Scanner Image

Give your virtual scanner a name and choose a virtualization platform.

Virtual Scanner Name
My Scanner

Choose a Virtualization Platform
VMware Workstation, Workstation Player, Fusion

Need help?
Click here for guidance

Choose an Asset Group
Windows Hosts

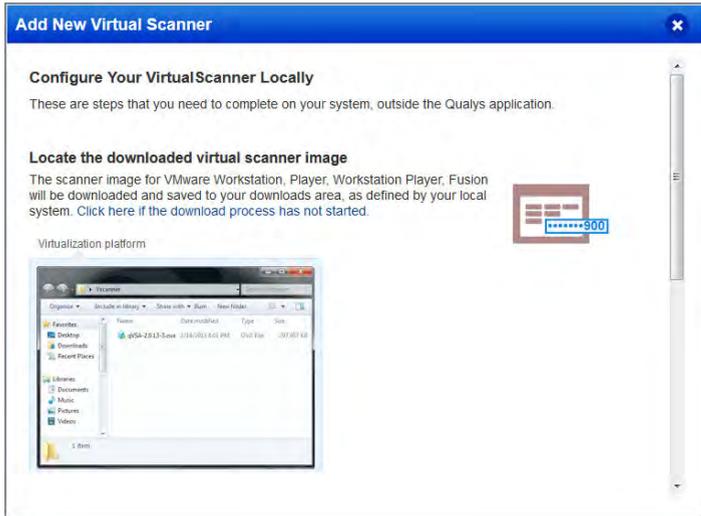
Close

Next

ステップ 3 - イメージのダウンロード

この手順は Scanner Appliance イメージダウンロード（つまり、VMware、Citrix XenServer 用など）がある仮想化プラットフォームに適用されます。クラウドプラットフォームを使用する場合次のステップに進みます。

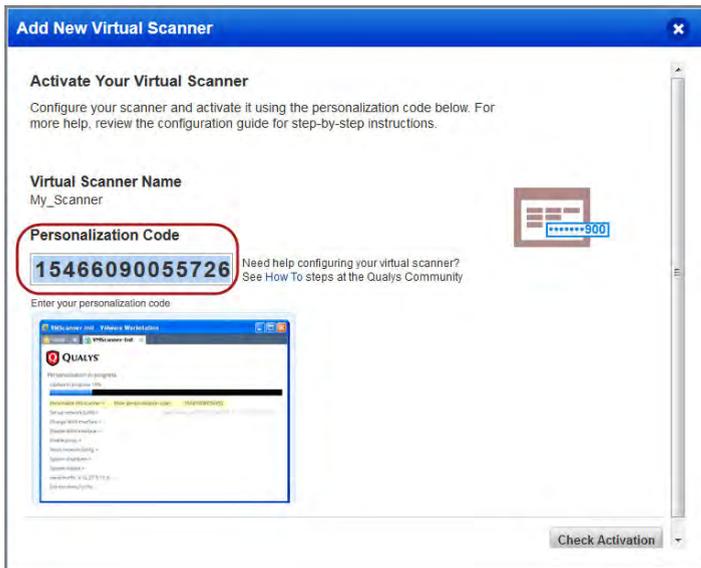
Virtual Scanner イメージのある場所（ローカルシステム上）を指定します。



KVM へのインポートに QCOW2 形式を検討する場合 OVA イメージファイルをダウンロードして、qemu-img ツールを使用して変換します。 [詳細](#)

ステップ 4 - パーソナル化コードを取得

コードを安全な場所に保存しておきます（後で使用します）。



ステップ 5 - プラットフォームの設定手順を完了

画面の「How to」リンク（パーソナル化コードのとなり）に従って、仮想化プラットフォームの詳しい手順を取得します。手順はプラットフォームによって少し異なります。

ステップ 6 - Scanner のパーソナル化

ローカルシステムまたはサーバ

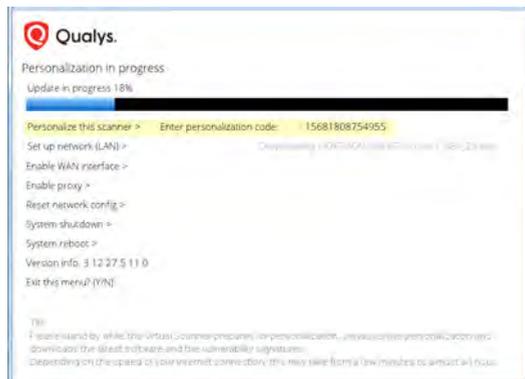
これらの手順は **Scanner Appliance** イメージ（つまり、VMware、Citrix XenServer など）がある場合に適用されます。これらの手順を完了するには、仮想化ソフトウェア上で当社の **Virtual Scanner Console** を使用します。

キーポイント - Virtual Scanner は DHCP に自動設定されています。静的 IP を使用する場合は、最初に「Set up network (LAN)」を選択します。 [詳細](#)



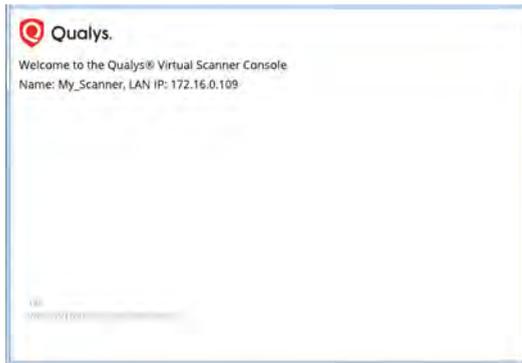
右矢印を押して「Personalize this scanner」を選択し、パーソナル化コードを入力します。

パーソナル化コードがない場合は、Qualys のページに移動し、「Scans」→「Appliances」のリストから取得します。



コードを入力するとアクティブ化プロセスが開始され、進行状況が表示されます。完了するまで、数分かかることがあります。

アクティブ化を完了し、最新のソフトウェアバージョンをダウンロードするには、**Virtual Scanner** を **Qualys** のクラウドセキュリティプラットフォームに接続する必要があります。



プロセスが完了すると、このスキャナの名前と IP アドレスが表示されます。以上で完了です。これで、アカウントに **Virtual Scanner** が追加されました。

アクティブ化の実行で問題が発生した場合は、[こちらをクリック](#)してください。

当社から詳細な手順とベストプラクティスを入手してください。

詳細

[Scanner Appliance FAQs](#)

[Configure a virtual scanner using VMware \(various products\)](#)

[Configure a virtual scanner using Microsoft Hyper-V](#)

[Configure a virtual scanner using VMware vSphere \(vCenter\)](#)

[Configure a virtual scanner using a laptop connected to the Internet \(WiFi\)](#)

クラウドプラットフォーム

これには、Amazon EC2、Microsoft Azure、Google Cloud Platform、OpenStack、OCI および OCI-Classic、ならびに Alibaba Cloud Compute が含まれます。Scanner Appliance インスタンス設定の一部として、クラウドプラットフォームにパーソナル化コードを入力します。当社から詳細な手順とベストプラクティスを入手してください。

詳細

[Configure a virtual scanner using Amazon EC2](#)

[Choosing the Correct Scanner AMI \(Amazon Machine Image\)](#)

[Scanning in Microsoft Azure](#)

[Virtual Appliance in Google Compute Cloud \(GCE\)](#)

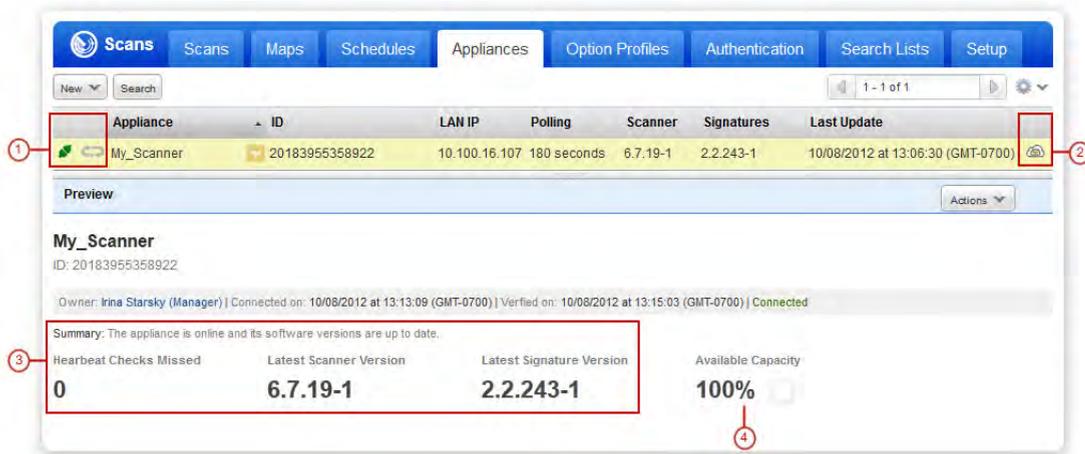
[Scanning in OpenStack](#)

[Deploy virtual scanner in Oracle Cloud Infrastructure \(OCI\)](#)

役立つその他の機能

Virtual Scanner の状態を確認します。「Scans」→「Appliances」に移動してスキャナを選択すると、プレビューパネルが表示されます。

ヒント - 新しいアプライアンスの追加後、Qualys ソリューションのユーザインタフェースに追加が反映されるまでには数分間を要することがあります。最新の詳細を表示するには、ブラウザの表示を定期的に更新してください。



1 - が表示されている場合は、Virtual Scanner の準備は整っています。この時点で内部スキャンを開始できます（このアイコンの横にあるビジューアイコンは、このスキャナを使用してスキャンを開始するまでグレーアウト表示になっています）。

2 - これは、仮想アプライアンスであることを示しています。

3 - 最新のソフトウェアバージョン。これらはアクティブ化処理の際にインストールされます。

4 - スキャンを開始するまで、使用可能な処理能力は 100% です。いつでもここで処理能力を確認することができます。

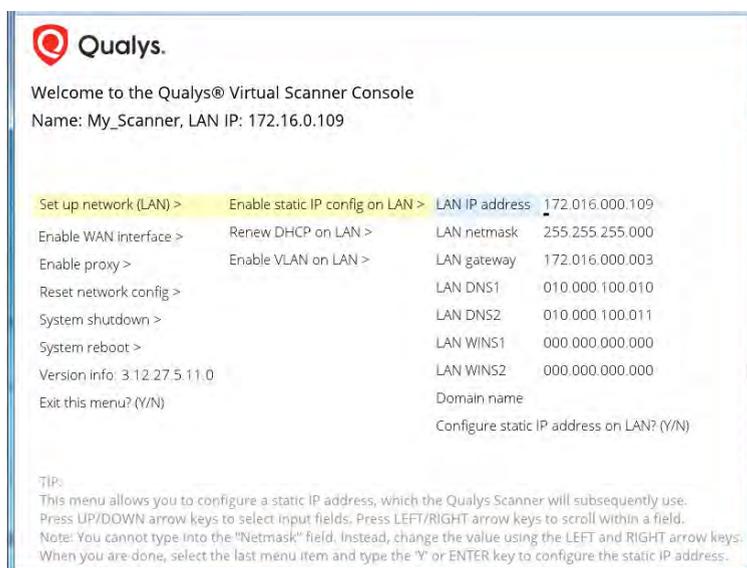
設定

場合によっては、スキャナの設定をカスタマイズし、Qualys のクラウドセキュリティプラットフォームと通信できるようにする必要があります。これは、アクティブ化を完了させる際に必要です。

ネットワーク設定

静的 IP アドレス、プロキシサーバ、VLAN タグ (802.1q トランクポート用) など、Virtual Scanner で選択できるネットワーク設定は複数あります。Virtual Scanner Console を使用して、ネットワーク設定を入力します。

スキャナのパーソナル化で問題が発生する場合は、まずネットワーク設定を行う必要があるかもしれません。



静的 IP アドレスの使用方法

アプライアンスに、DHCP ではなく静的 IP アドレスを設定することもできます。

- Virtual Scanner Console を使用して、メインメニューに進みます。
- 「Set up network (LAN)」を選択します。
- 右矢印を押して、「Enable static IP config on LAN」を強調表示します。
- 右矢印を押します。
- 設定を入力します。

設定を入力するには、上矢印または下矢印を押して、入力するフィールドを選択します。フィールド内でカーソルを移動するには、右矢印または左矢印を押します。入力が終了したら、一番下にある項目（例：「Configure static IP address on LAN?」）を選択し、「Y」を入力して確定します（または「N」を入力してキャンセルします）。

Amazon EC2 を使用して静的 IP を設定する場合は、[こちらをクリック](#)してください。

LAN 上で VLAN を有効化（ネイティブ/デフォルト VLAN）

ネイティブ VLAN インタフェースは、デフォルトで DHCP 設定で設定されます。静的 VLAN 設定を希望する場合は、続行する前に LAN 上で静的 IP 設定が有効化され保存されていることを確認します。

LAN インタフェースを 802.1q トランクポートに接続し、Virtual Scanner が LAN デフォルトネットワーク上で VLAN タグを使用する必要がある場合、Virtual Scanner Console で「Enable VLAN on LAN」を選択します。使用する VLAN タグ番号（1～4094）を入力します。

VLAN および静的ルートの設定（Qualys UI）

VLAN および静的ルートの設定は、Amazon EC2/VPC、Microsoft Azure および Google Cloud Platform などのクラウドプラットフォームを除く、すべての Virtual Scanner ディストリビューションでサポートされています。

Qualys にログインして、アプライアンスリスト（「Scans」→「Appliances」）に移動し、アプライアンスの設定を編集します。最新のディストリビューションを使用している場合、それぞれの Virtual Scanner Appliance に追加できる VLAN および静的ルートは最大で 4,094 です。スキャナイメージ qVSA-2.0.13-1以降を使用して展開していれば、Virtual Scanner は最新です（これよりも古いバージョンである場合、追加できる VLAN および静的ルートは 99 までです）。

これらの設定が表示されない場合は、アカウントで VLAN トランク機能を有効にする必要があります。この機能を有効にするには、サポートまたはテクニカルアカウント担当者までお問い合わせください。

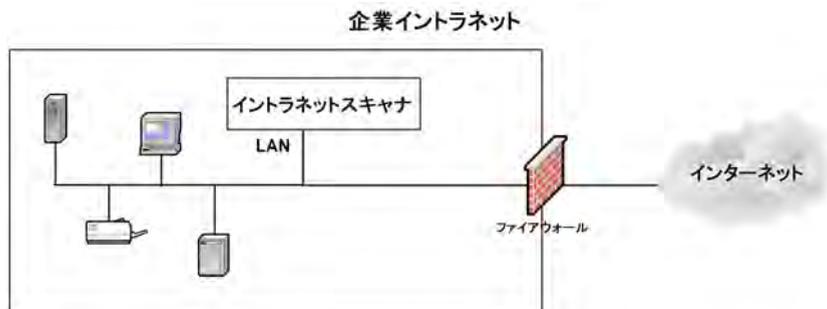
Proxy configuration

Scanner では、認証（ベーシック認証または NTLM 認証）を使用する、または使用しないプロキシサポートが可能です。プロキシサーバに静的 IP アドレスを割り当て、透過型 SSL トンネルを許可している必要があります。SSL ブリッジなどで実装されるプロキシレベルのターミネーションはサポートされません。プロキシサーバの IP アドレスを動的に割り当てるネットワーク環境の場合、スキャナでは、プロキシサーバはサポートされていません。SOCKS プロキシはサポートされていません。

手順 Virtual Scanner Console にアクセスします。「Enable proxy」に移動し、右矢印を押して、プロキシ設定を入力します。プロキシサーバとして IPv4 アドレスまたは FQDN のいずれかを入力できます。FQDN オプションが表示されない場合スキャナのソフトウェアバージョンが最新であることを確認してください。

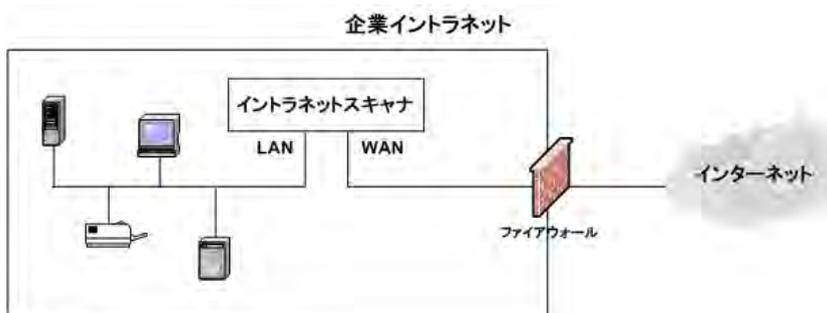
分離ネットワーク設定

デフォルトでは Scanner LAN インタフェースは、管理トラフィック（ソフトウェアアップデート、ヘルスチェック、スキャンデータのアップロード）を含む、すべてのトラフィックを Qualys Cloud Platform にサービスします。



Virtual Scanner Console を使用して WAN インタフェースを設定することにより、Scanner に分離ネットワーク設定を設定するオプションがあります。これにより、インターネットへの直接アクセスのないネットワークに対するサポートが可能になります。分離ネットワーク設定により、WAN インタフェースを使用して内部 LAN トラフィックを分離することにより、スキャン済データおよび内部ターゲットが安全に保たれます。

一度設定すると、管理トラフィックは WAN インタフェースを介してルーティングされ、トラフィックスキャンは LAN インタフェースを介してルーティングされます。内部トラフィックは WAN インタフェースにルーティングやブリッジされず、管理トラフィックは LAN インタフェースにルーティングやブリッジされません。



分離ネットワーク設定を行う前に、次のヒントやベストプラクティスを確認してください。

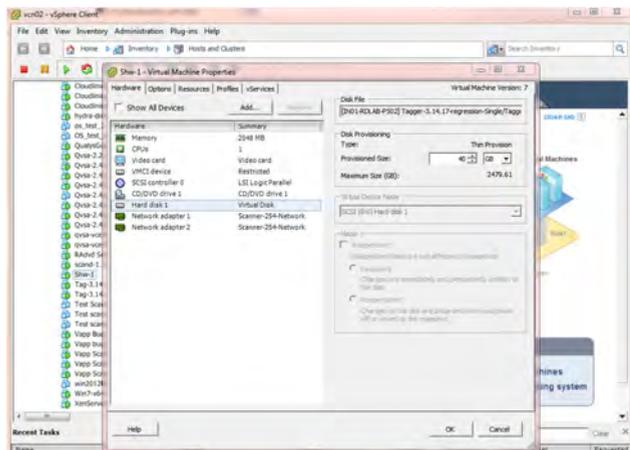
- Virtual Scanner の LAN と WAN インタフェースの両方でネットワーク接続が適切に設定されていることを確認します。
- まず、Virtual Scanner の LAN インタフェースに DHCP または静的 IP アドレスを設定する必要があります。
- 同じサブネット上に LAN と WAN のインタフェースを設定しないようにしてください。そのような設定には対応していません。

手順 Virtual Scanner Console にアクセスします。「Enable WAN interface」に移動し、右矢印を押して、必要な設定を入力します。ソフトウェア更新と稼働状態チェックのすべてのトラフィックは WAN インタフェース経由でルーティングされ、スキャントラフィックは LAN インタフェース経由でルーティングされます。

ディスクのリサイズ

Scanner Appliance インスタンスのディスクサイズを、いつでも必要なだけ増やすことができます。インスタンスを停止し、Virtual Machine 設定で Hard Disk/Storage オプションを見つけて、ディスクのサイズを増やします（サイズの削減はサポートされていません）。設定を保存してスキャナを起動します。スキャナインスタンスは新しいディスクサイズになって起動します。

これは VMware ESXi/vCenter プラットフォームの例です。



イメージの別の形式への変換

Scanner のイメージディスクには VMDK および VHD 形式があります。これらは、qemu-img ツールでサポートされているいずれの形式にも変換することができます。たとえば VMDK または VHD を QCOW2 または RAW に変換することができます。以下のコマンドにより、サポートされる形式の一覧が表示されます。

```
qemu-img -h
```

以下のステップでは、OVA ファイル（VMDK ディスク形式）を QCOW2 に変換して、Linux/RedHat Enterprise 仮想マシンとして、KVM ハイパーバイザにインポートします。

- 1) Linux システムで、qemu-img ツールをインストールします。
- 2) Qualys（例、qVSA.i386-2.2.27-1.ova）から Standard イメージを OVA 形式でダウンロードします。
- 3) OVA から .vmdk ディスクイメージファイルを展開する方法は以下のとおりです。

```
#] tar xvf qVSA.i386-2.2.27-1.ova
```

これにより同じ場所に qVSA.i386-2.2.27-1-disk1.vmdk ファイルが展開されます。

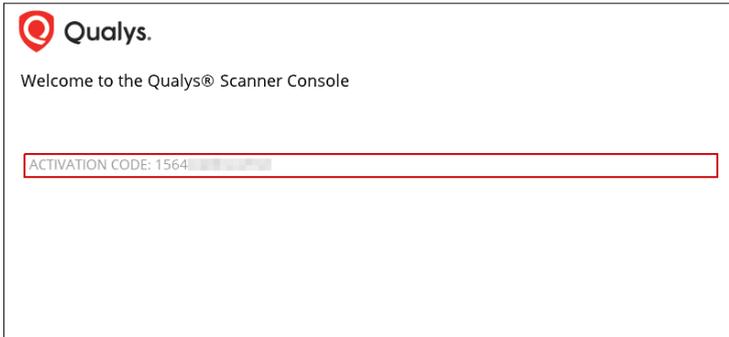
- 4) 次のようにして、.vmdk ディスクイメージを qcow2 形式に変換します。

```
#] qemu-img convert -f vmdk -O qcow2 qVSA.i386-2.2.27-1-disk1.vmdk
qVSA.i386-2.2.27-1-disk1.qcow2
```

- 5) Linux/RedHat Enterprise 仮想マシンとして、qVSA.i386-2.2.27-1-disk1.qcow2 を KVM にインポートします。

トラブルシューティング

アクティブ化コードが表示される理由



Scanner Console ではアクティブ化コードが表示される場合もあります。

- Qualys ポータル UI を使用してアクティブ化コードを入力する前に、スキャナに電源を入れた。
- Qualys ポータル UI を使用して間違ったアクティブ化コードを入力した。つまり、スキャナには別のアクティブ化コードがある。
- アクティブ化手順に続いてアクティブ化コードを入力したが、間違った Qualys クラウドプラットフォームを使用した。たとえば、スキャナが US プラットフォーム 2 の代わりに US プラットフォーム 1 にライセンス許可されている場合です。

Communication Failure メッセージ

「COMMUNICATION FAILURE」メッセージは、スキャナと Qualys クラウドプラットフォームの間でネットワークの断絶がある場合に表示されます。

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が停止している、インターネット接続が何らかの理由で失われている、またはスキャナと Qualys クラウドプラットフォームの間のネットワークデバイスがダウンしていることが考えられます。

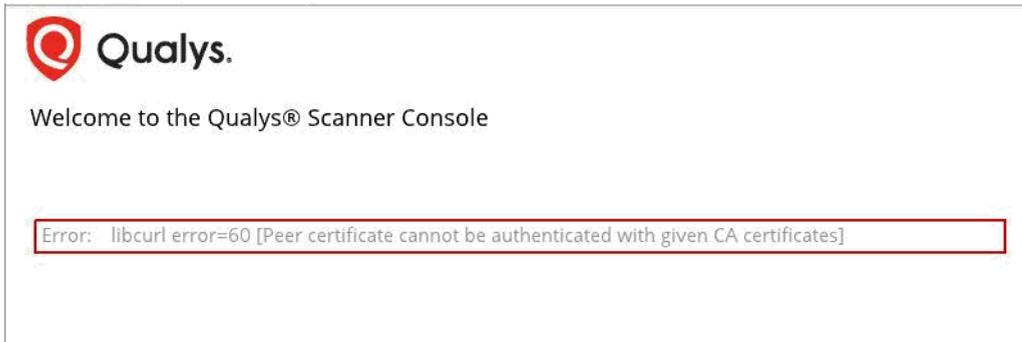
ネットワークの断絶の後に発生したイベントシーケンスに注意してください。

- スキャナでスキャンが実行されていない場合：スキャナが Qualys クラウドプラットフォームへ次回のポーリングリクエストを送信すると、ポーリングリクエストが失敗して「COMMUNICATION FAILURE」メッセージが表示されます。
- スキャナでスキャンが実行されている場合：スキャンのタイムアウト後、「COMMUNICATION FAILURE」メッセージが表示されます。この場合、正確な結果を確保するため、実行中のスキャンをキャンセルして再開します。

ネットワークの断絶が解決されると、分かりやすいスキャナの名前と IP アドレスが表示され、新規のスキャンを開始できます。

「COMMUNICATION FAILURE」メッセージは、スキャナから Qualys クラウドプラットフォームへのポーリングリクエストが次に成功するまで表示されます。次回のポーリングリクエストのスケジュールによっては、ネットワークが復旧してからスキャナがオンラインに戻るまでに遅延が生じることがあります。スキャナにプロキシ設定がある場合、プロキシサーバが通信を処理する時間もかかります。

アプライアンス設定エラー



アプライアンス設定エラーはスキヤナが Qualys クラウドプラットフォームに接続できなかったことを示します。

重要！スキヤナはエラーが解決するまで機能しません。

エラー一覧

一般

Qualys クラウドプラットフォームからの HTTP リクエストに対する応答なし

無効なプロキシ IP

無効なプロキシ設定

libcurl error=7 「ホストへの接続失敗」
(libcurl エラーコードの完全なリストについては、curl (1) マニュアルページを参照してください)

予期しない QG HTTP/404
(QG は Qualys クラウドプラットフォームを表す)

予期しない HTTP/407 (プロキシ認証エラー)

LAN 関連

LAN インタフェースに障害

LAN インタフェースが通信していない

LAN に IPv4 アドレスがない

LAN に DNS サーバがない

LAN DNS サーバが Qualys クラウドプラットフォームの URL を解決できない

LAN に IPv4 のデフォルトゲートウェイがない

無効な LAN IP 設定

LAN DNS サーバがプロキシ URL を解決できない

WAN 関連

WLAN インタフェースに障害

WAN インタフェースが通信していない

WAN に IPv4 アドレスがない

WAN に DNS サーバがない

WAN DNS サーバが Qualys クラウドプラットフォームの URL を解決できない

WAN に IPv4 のデフォルトゲートウェイがない

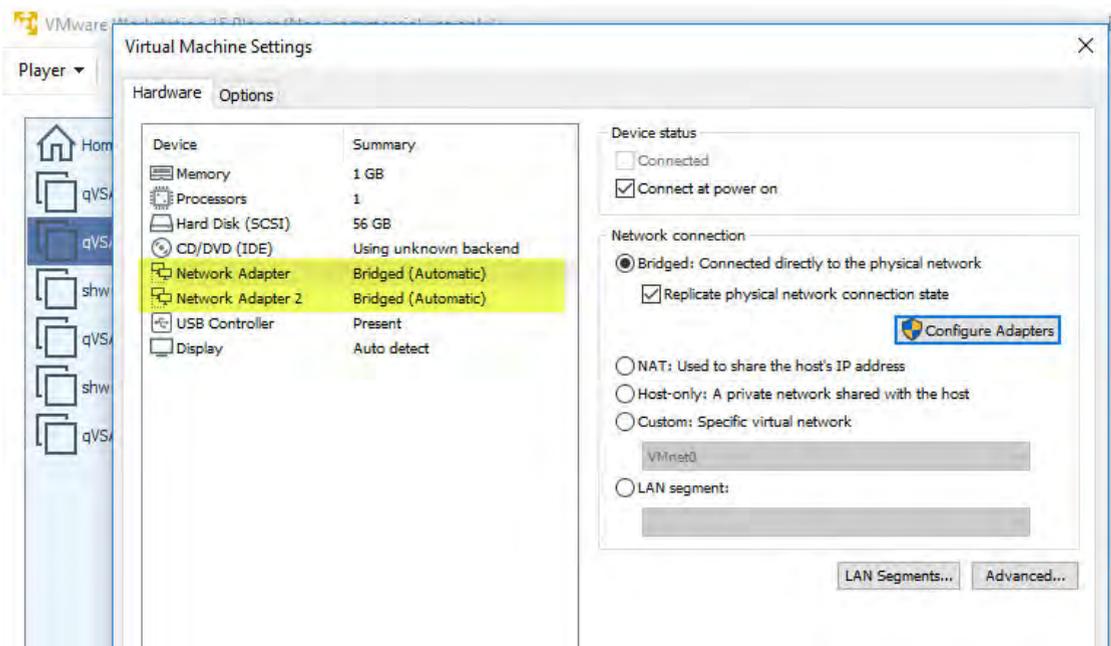
無効な WAN IP 設定

WAN DNS サーバがプロキシ URL を解決できない

スキャナに返された IP が不正で接続または表示に問題がある場合

Virtual Scanner 用に選択したネットワークアダプタを変更する必要がある場合があります。

仮想化ソフトウェアにより、正しいネットワークアダプタが適切に設定されたアプライアンスのインスタンスが自動的に作成されます。これらのインタフェースは Network Adapter と Network Adapter 2 になります。デフォルトでは、どちらのインタフェースもタイプは「Bridged (Automatic)」になります。これは、ネットワークアダプタは自動で選択されるということを意味します。



複数のネットワークアダプタを搭載したホスト上に仮想マシンをインストールしている場合は、自動が設定されていることで、不適切なアダプタが選択される可能性があります。自動で選択されたネットワークアダプタを場合によっては変更する必要があります。ネットワークアダプタを配置するネットワークに基づいて仮想マシンを使用するよう、ネットワークアダプタを変更します。

最初に、ホスト上にインストールしたネットワークアダプタのうち、どれが仮想マシンに適切であるかを判断します。Windows の場合は、IP ログをすべての詳細情報と一緒にダンプ表示し、ホストに属している IP のネットワークアダプタ名を確認します。

その後、「Virtual Machine Settings」を表示して、自動でブリッジモードにするホストのネットワークアダプタを選択します。ここでは、VMware Player の例を紹介します。「Configure Adapters」ボタンをクリックすると、自動ブリッジで使用できるネットワークアダプタが表示されます。

トラブルシューティング
スキャナに返された IP が不正で接続または表示に問題がある場合

