Securing Microsoft Azure with Qualys

March 12, 2020
# Table of Contents

**About This Guide**.......................................................................................................................... 5
  - About Qualys ................................................................................................................................. 5
  - Qualys Support ............................................................................................................................ 5

**Introduction**................................................................................................................................. 6
  - Qualys Integrated Security Platform .......................................................................................... 6
  - Pre-requisites .............................................................................................................................. 7

**Automate Asset Inventory**........................................................................................................... 9
  - Deploying Azure Connector ......................................................................................................... 9
    - Pre-requisites .......................................................................................................................... 9
    - Creating Azure Connector with AssetView ............................................................................. 10
    - Set up Authentication Details ............................................................................................... 12
  - How Does Azure Connector Work? ............................................................................................ 16
  - Viewing Imported Assets ............................................................................................................ 16
  - Azure Metadata ......................................................................................................................... 17
    - AssetView Connector & Qualys Cloud Agent Metadata ....................................................... 17
    - Scanner Metadata .................................................................................................................. 19
  - Azure APIs Used by Azure Connector to Discover Assets ....................................................... 20
    - Resource Groups - List ........................................................................................................... 20
    - Virtual Machines - List ......................................................................................................... 20
  - Qualys APIs for Azure Connectors ............................................................................................ 20

**Scanning in Azure Environments**................................................................................................... 21
  - Single VNet Single Region ......................................................................................................... 21
  - Single VNet Single Region Multiple Scanners ........................................................................ 22
  - Multiple VNet Single Region ...................................................................................................... 23
  - Multiple VNet Multiple Region .................................................................................................. 24
  - Non Peered VNets ..................................................................................................................... 25

**Deploying Sensors**...................................................................................................................... 26
  - Deploying Scanners in Azure Platform ....................................................................................... 26
    - Cost and Licenses .................................................................................................................... 26
    - Deployment Recommendations for Scanners ......................................................................... 27
    - What do I Need? ....................................................................................................................... 27
  - Deploying Qualys Scanner Appliance ......................................................................................... 28
  - Deploying Scanners in Private Cloud Platform .......................................................................... 39
    - Deploying Qualys Scanners (using CLI) .................................................................................. 39
    - Using Azure GUI to Create Qualys Image from VHD file (Optional) .................................. 43
  - Deploying Qualys Cloud Agent .................................................................................................. 45
    - Deploy Qualys Cloud Agent from Azure Security Center .................................................... 45
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedding Qualys Cloud Agent as a part of Golden Machine Image</td>
<td>56</td>
</tr>
<tr>
<td>Deploy Qualys Cloud Agent via Azure ARM Template</td>
<td>56</td>
</tr>
<tr>
<td>Deploy Qualys Cloud Agent via Other Tool Sets</td>
<td>56</td>
</tr>
<tr>
<td><strong>Scan Assets</strong></td>
<td>60</td>
</tr>
<tr>
<td>Azure Scan Checklist</td>
<td>60</td>
</tr>
<tr>
<td>Tips and Best Practices</td>
<td>65</td>
</tr>
<tr>
<td>Internal Scanning using Virtual Scanner Appliance</td>
<td>65</td>
</tr>
<tr>
<td>Internal Network Scanning using Qualys Cloud Agent</td>
<td>68</td>
</tr>
<tr>
<td>Perimeter Scanning using Qualys External Scanners</td>
<td>68</td>
</tr>
<tr>
<td>Cloud Inventory and Security Assessment</td>
<td>71</td>
</tr>
<tr>
<td>Cloud Inventory</td>
<td>71</td>
</tr>
<tr>
<td>Cloud Security Assessment</td>
<td>72</td>
</tr>
<tr>
<td>Securing Web Applications</td>
<td>73</td>
</tr>
<tr>
<td>Securing Containers</td>
<td>74</td>
</tr>
<tr>
<td>Deploying Container Sensor</td>
<td>75</td>
</tr>
<tr>
<td><strong>Analyze, Report &amp; RemEDIATE</strong></td>
<td>76</td>
</tr>
<tr>
<td>How to Query Azure Assets</td>
<td>76</td>
</tr>
<tr>
<td>View Asset Details Anytime</td>
<td>77</td>
</tr>
<tr>
<td>Save Query</td>
<td>77</td>
</tr>
<tr>
<td>Download and Export Results</td>
<td>78</td>
</tr>
<tr>
<td>Create Widget</td>
<td>78</td>
</tr>
<tr>
<td>Creating Reports</td>
<td>79</td>
</tr>
<tr>
<td>Dynamic Tagging Using Azure Attributes</td>
<td>80</td>
</tr>
<tr>
<td><strong>Manage Assets Using Qualys</strong></td>
<td>81</td>
</tr>
<tr>
<td>Setting up Qualys Configurations</td>
<td>81</td>
</tr>
<tr>
<td><strong>Common Questions</strong></td>
<td>84</td>
</tr>
</tbody>
</table>
About This Guide

Welcome to Qualys Cloud Platform and security scanning in the Cloud! We’ll help you get acquainted with the Qualys solutions for scanning your Cloud IT infrastructure using the Qualys Cloud Security Platform.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com

Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions are answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at www.qualys.com/support/
Introduction

Welcome to Qualys Cloud Platform that brings you solutions for securing your Cloud IT Infrastructure as well as your traditional IT infrastructure. In this guide we’ll be talking about securing your assets in Microsoft Azure infrastructure using Qualys.

Qualys Integrated Security Platform

With Qualys Cloud Platform you get a single view of your security and compliance - in real time. If you’re new to Qualys we recommend you to visit the Qualys Cloud Platform web page to know more about our cloud platform.
Azure Cloud Terminologies

Microsoft Azure - The Microsoft cloud platform, a growing collection of integrated services including Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) offerings. [Learn more]

Azure Resource Manager - Azure Resource Manager enables you to work with the resources in your infrastructure solution as a group. You can deploy, update, or delete all the resources for your solution in a single, coordinated operation. You use a template for deployment and that template can work for different environments such as testing, staging, and production. [Learn more]

Resource Group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more]

Resource Manager Template - A JavaScript Object Notation (JSON) file that defines one or more resources to deploy to a resource group. It also defines the dependencies between the deployed resources. The template can be used to deploy the resources consistently and repeatedly. [Learn more]

Microsoft Azure Cloud Computing Terms - Microsoft Azure portal has a dictionary of common cloud computing terms relevant to their cloud based services. This is especially useful if you are new to Microsoft Azure. [Learn more]

Securing Azure Essentials - IaaS and PaaS

Qualys integrates with Microsoft Azure Resource Manager (ARM) to discover assets using a Microsoft ARM API. This integration automatically detects and synchronizes changes to virtual machine instance inventories within Azure Cloud Platform. Virtual machines are tracked by virtual machine Id within Qualys even as their IP addresses change over time.

Pre-requisites

- **Qualys Applications:** Vulnerability Management (VM), Policy Compliance (PC) or Security Configuration Assessment (SCA), Cloud Agent (CA)
- **Qualys Sensors:** Virtual Scanner Appliances, Cloud Agents, as desired
- **Qualys Virtual Scanner Appliance:** Virtual machine must be able to reach the Qualys Cloud Platform over HTTPS port 443
- **Scanner personalization code (14 digits) used to deploy Virtual Scanner Appliance:** This is obtained from your Qualys account as described in Add New Virtual Scanner in Qualys
- **Qualys user account:** Must have Manager or Unit Manager role
It's easy to get started

You might already be familiar with Qualys Cloud Suite, its features and user interface. Here are the links to video libraries -

- Vulnerability Management
- Policy Compliance
- CloudView
- Web Application Scanning
- Cloud Agent
- Integrate Qualys into Azure Security Center

Here are the links for some helpful resources -

- Qualys Training | Free self paced classes, video series, online classes
- Qualys Documentation | Getting started guides, quick references, API docs
- Qualys Community | Learn from the Project Managers, Subject Matter Experts and other Qualys customers
- Qualys Blog | Get latest updates and Helpful hints

Quick Steps: Securing Azure

Here's the user flow for securing Azure using Qualys.

1. **Automate Asset Inventory**
   Sync inventory and metadata for an Azure virtual machine by setting up AssetView Azure Connector

2. **Design Sensor Deployment Strategies**
   Analyze Environment and deployment strategies for Cloud Agent and Virtual Scanner Appliance

3. **Deploy Sensors**
   Install Scanner Appliance and/or Cloud Agents

4. **Scan Assets**
   Launch scans targeting all assets or specific assets you're interested in

5. **Analyze, Report & Remediate**
   View dynamic dashboards, create custom widgets and run reports

6. **Cloud Inventory and Security Assessment**
   Continuously inventory and assess your Azure cloud workloads

7. **Securing Containers**
   Identify Container Hosts, Registries, and CICD Pipelines and Deploy Container Sensors

8. **Securing Web Applications**
   Configure Qualys Web Application Scanning to scan your applications
Automate Asset Inventory

Deploying Azure Connector

Configure Microsoft Azure connectors for gathering resource information from your Microsoft Azure account. You can create Azure Connector from AssetView and CloudView which is explained after pre-requisites. It just takes a couple of minutes.

Let us see what permissions are needed to create Azure connector.

Pre-requisites

Before you create an Azure connector, ensure that you have the following permissions:

- **Assign Azure Active Directory permissions** to register an application with your Azure Active Directory

- **Checking Azure Subscription Permissions** to assign the application to a role in your Azure subscription

Assign Azure Active Directory permissions

Navigate to Azure Active Directory > User Settings and then ensure that the App registrations are allowed for your Azure subscription.

If you Azure subscriptions has the app registrations setting set to No, you need to check whether your account is an admin or user for the Azure AD account.

To check if your account is an admin, go to Overview and look at your user information.
If your account is assigned to the User role, but the app registration setting is restricted to admin users, you are not permitted to register new apps. In such case, ask your administrator to either assign you to the global administrator role, or to enable users to register apps.

**Checking Azure Subscription Permissions**

In your azure subscription, your account must have Owner access role to assign an AD app to a reader role. If your account is assigned to the Contributor role, you do not have adequate permissions and receives an error when attempting to assign the service principal to a role.

To know the role assigned to you, select your account (refer image) and select My permissions. From the Subscription drop-down list, select the subscription for which you would want to check permissions and then click the “Click here to view complete access details for this subscription” link.

![Image](image.png)

**Creating Azure Connector with AssetView**

1) Login to the Qualys Cloud Platform and pick the AssetView app. Go to Connectors > Azure tab, select Create Azure Connector and our wizard walks you through the steps.

**Tip** - We recommend you create at least one generic asset tag (for example, Azure) and let the connector automatically apply that tag to all imported assets. You can add more tags to your Azure assets based upon the discovered Azure metadata.

2) Enter a name and description (optional) for your connector.
3) Select the account type: Global or GovCloud. You can choose only one account type per connector.

4) Set up Authentication Details and copy/paste the authentication details into the form.

5) Configure the asset tags in Tags and Activation for scanning if you plan to use a pre-authorized scanner appliance.

6) Click Create Connector.

That’s it! The connector establishes a connection with Microsoft Azure to start scanning Microsoft Azure resources for security issues using the Qualys Cloud Platform.
Set up Authentication Details

This section helps you to gather the parameters required to create Azure Connector.

Create Application and get Application ID, Directory ID

Create application in Azure Active Directory and you can then note the application ID.

1) Log on to the Microsoft Azure console and press Azure Active Directory in the left navigation pane.

2) Click App Registrations > New registration.

3) Provide the following details:
   - Name: A name for the application (For example, My_Azure_Connector)
   - Supported account types: Select Accounts in any organizational directory.

4) Click Register. The newly created application is displayed with its properties. Copy the Application (client) ID and Directory (tenant) ID and paste it into the connector details.
Generate Authentication Key

Provide permission to the new application to access the Windows Azure Service Management API and create a secret key.

1) Select the application that you created and go to API permissions > Add a permission.
2) Select Azure Service Management API in Microsoft APIs for Request API permissions.

3) Select user impersonation permission and click Add permissions.

4) Select the application that you created and go to Certificates and Secrets > New client secret.
5) Add a description and expiry duration for the secret key (recommended: Never) and click Add.

![Add a client secret](image)

6) The value of the key appears in the Value field.

Copy the key value at this time. You won’t be able to retrieve it later. Paste the key value as Authentication Key into the connector details. You need to provide the key value with the application ID to log on as the application. Store the key value where your application can retrieve it.
Acquiring Subscription ID
Grant permission for the application to access subscriptions. Assign a role to the new application. The role you assign defines the permissions for the new application to access subscriptions.

1) On the Azure portal, navigate to Subscriptions.

2) Select the subscription for which you want to grant permission to the application and note the subscription ID. To grant permission to the application you created, choose Access Control (IAM).

3) Go to Add > Add a role assignment. Pick a Reader role. A Reader can view everything, but cannot make any changes to the resources of a subscription.

4) Select Azure AD user, group, or application in Assign Access to drop-down.

5) Type the application name in Select drop-down and select the application you created.

6) Click Save to finish assigning the role. You’ll see your application in the list of users assigned to a role for that scope.
7) Copy the subscription ID you noted and paste it into the connector details in the Qualys Azure Connector screen and then click Create Connector.

**How Does Azure Connector Work?**

**Asset Discovery**: The Azure connector performs asset discovery for your cloud with its continuous synchronization mechanism. The connector synchronizes every 4 hours with the Azure account and pulls in all virtual machines (After the connector run, if a virtual machine is found as terminated, connector stores such virtual machine with “DELETED” state.).

Azure retains the terminated virtual machines for only about 15 minutes. However, Qualys retains record and details of all the terminated virtual machines.

**Synchronization of Assets**: Adds the assets to your Qualys account. Except for assets with errors (as such assets are dropped off), all other assets are added to the Qualys account.

**Viewing Imported Assets**

![Image of Azure Connector](image)

The Azure connector starts pulling the virtual machines once you finish the connector creation. Let’s check out the different information we display once the connector run is complete.

1. **Asset Count** - The Asset count column shows the assets discovered and synchronized in the latest Azure connector run.

2. **Synchronized Assets** - In the Asset count column, the green portion represents assets synchronized. Synchronized count represents assets that are successfully processed at Qualys.

3. **Show Assets** - Total count of assets discovered by the connector over its span of time.
Assets with Error - The Asset count column may also show a portion in red which represents assets with errors. Assets with errors are those which have encountered issues while being processed at Qualys.

You can view the assets that are collected by connector by navigating to AssetView. The Azure VM Information tab of Asset details page displays the Azure instance metadata collected. Here is the sample screen shot that displays the information we collect.

Once the Azure virtual machines are discovered, you are ready to start scanning and securing your Microsoft Azure infrastructure!

Azure Metadata
This section provides information on cloud provider metadata provided by Qualys Cloud Agent, AssetView Connector and Qualys Scanner

AssetView Connector & Qualys Cloud Agent Metadata
General:
- VM ID (compute.vmId)
- VM Name(compute.name)
- Platform /OS Type (compute.osType)
- Size (compute.vmSize)
- Image Offer (compute.offer)
- Image Publisher (compute.publisher)
- Image Version (compute.version)
- Subscription ID (compute.subscriptionId)
- Location (compute.location)
- Resource Group Name (compute.resourceGroupName)
- VM State (Only Running for QCA data collection)

Network:
- Private IP Address (network.interface.ipv4.ipaddress.privateIpAddress)
- Public IP Address (network.interface.ipv4.ipaddress.publicIpAddress)
- MAC Address (network.interface.macAddress)
- Subnet (network.interface.ipv4.subnet.address)

Azure VM Tags:
- LifeCycle (compute.tags)
- Owner (compute.tags)
- Department (compute.tags)
Scanner Metadata

Scanner metadata for authenticated scans on Azure Linux virtual machine– QID 45389

Computer:
- azEnvironment
- location
- name
- offer
- osType
- placementGroupId plan
  - name
  - product
  - publisher
- platformFaultDomain
- platformUpdateDomain
- providerpublicKeys
  - keyData
  - path
  - publisher
- resourceGroupName
- sku
- subscriptionId
- tags
- version
- vmId
- vmScaleSetName
- vmSize
- zone

Network Interface ipv4:
- ipAddress
- privatelIpAddress
- publicIpAddress
- subnet
- address
- prefix

Network Interface ipv6:
- ipAddress
- macAddress

**Azure APIs Used by Azure Connector to Discover Assets**

Qualys uses Azure APIs to get all resource groups for a subscription and list all virtual machines for the specified resource group.

**Resource Groups - List**
https://docs.microsoft.com/en-us/rest/api/resources/resourcegroups/list

**Virtual Machines - List**
https://docs.microsoft.com/en-us/rest/api/compute/virtualmachines/list

**Qualys APIs for Azure Connectors**

You can perform various Azure connector operations through API as well. For detailed information on using Qualys APIs related to Azure, see the Asset Management and Tagging API v2 User Guide.

Here are some useful Azure connector APIs:

**Create Azure Connector**
https://qualysapi.qualys.com/qps/rest/2.0/create/am/azureassetdataconnector

**Get Host Asset Info (get the metadata of an Azure instance)**
https://qualysapi.qualys.com/qps/rest/2.0/get/am/hostasset/<id>
Scanning in Azure Environments

Let us get familiar with few terms in networking basics.

**VNet**: An Azure Virtual Network (VNet) is a representation of your own network in the cloud. It is a logical isolation of the Azure cloud dedicated to your subscription. Each VNet you create has its own CIDR block and can be linked to other VNets and on-premises networks as long as the CIDR blocks do not overlap.

**VNet peering**: A mechanism that connects two virtual networks (VNets) in the same and/or different region through the Azure backbone network. Once peered, the two virtual networks appear as one for all connectivity purposes.

**Single VNet Single Region**

Scanners need to be configured to communicate to Qualys Cloud Platform over https (via Network security groups and proper routing).
**Single VNet Single Region Multiple Scanners**

Based on number of virtual machines and scan frequency, multiple scanners might be required to scan multiple machines in a VNet. You can add more scanners based on requirements.

Scanners needs to be configured to communicate to the Qualys Cloud Platform over https (via Network security groups and proper routing).
Multiple VNet Single Region

A single Scanner can reach multiple virtual machines in a peered VNets. Based on number of machines and scan frequency, multiple scanners might be required to scan multiple virtual machines across Peered VNets in a region.

Scanners needs to be configured to communicate to the Qualys Cloud Platform over https (via Network security groups and proper routing).
Multiple VNet Multiple Region

Azure allows peering of VNets across region hence a single scanner can reach virtual machines in different VNets in different regions. Based on number of machines and scan frequency, multiple scanners might be required to scan multiple virtual machines across Peered VNets in different regions.

Scanners needs to be configured to communicate to the Qualys Cloud Platform over https (via Network security groups and proper routing).
Non Peered VNets

Scanners reachability is curtailed if the VNets are not peered and hence cannot reach the virtual machines in non-peered VNets and launch a scan.

Scanners needs to be configured to communicate to the Qualys Cloud Platform over https (via Network security groups and proper routing).


Deploying Sensors

Qualys sensors, a core service of the Qualys Cloud Platform, make it easy to extend your security throughout your global enterprise. These sensors are remotely deployable, centrally managed and self-updating. They collect the data and automatically beam it up to the Qualys Cloud Platform, which has the computing power to continuously analyze and correlate the information in order to help you identify threats and eliminate vulnerabilities.

Prior to scanning, you need to deploy sensors. Depending on your preference, you could deploy pre-authorized scanner appliance or Qualys Cloud Agent. Let’s go through the steps involved in deploying these sensors.

Deploying Scanners in Azure Platform

Deploying Scanners in Private Cloud Platform

Deploying Qualys Cloud Agent

- Virtual Scanner Appliances
  Remote scan across your networks - hosts and applications
  Applications: VM, PC, SCA

- Cloud Agents
  Continuous security view and platform for additional security solutions
  Applications: CA (required), VM, PC, SCA

- Internet Scanners
  Perimeter scan for edge facing IPs and URLs
  Applications: VM, PC, SCA

Deploying Scanners in Azure Platform

Cost and Licenses

Qualys Virtual Scanner Appliance is available as an Image at Azure Marketplace, ready for customers to launch onto Azure Virtual Machines. There are two aspects to consider:

- Qualys costs for the virtual scanner license subscription
- Azure costs for the computing resources to run the appliance as a virtual machine

Qualys Cost

You need to acquire a Qualys license for each virtual scanner appliance Instance you would like to run. This license is acquired from Qualys, not from Azure, and our scanner appliances are listed at Azure Marketplace with a BYOL (i.e., “bring your own license”) model accordingly. Each Qualys Virtual Scanner Appliance profile that you define in the Qualys Cloud Platform UI consumes a single virtual scanner appliance license. If you
delete a virtual scanner appliance profile from your Qualys subscription, that license is freed up and immediately available for re-use. Contact your Qualys technical account manager or Qualys reseller for a pricing quotation or to request an evaluation.

Azure Cost

For each virtual scanner appliance, virtual machine is launched into one of your own Azure Subscriptions. You are responsible for paying Azure for the costs of running the appliance. Those costs include:

- Compute Capacity based upon size
- Storage - Data transfer IN/OUT

The compute capacity charges (i.e., CPU, RAM) are overwhelmingly the largest part of the costs to run an Instance. Note that you are not required to keep your scanner appliance(s) running at all times. Any hours during which your virtual machine is stopped, is incur only perGB provisioned storage charges. For those able to spend a little more upfront, Azure virtual machines can be reserved in advance by financially committing for one or three years to save. However, scanners should be turned on for at least several hours per week in order to ensure that they stay up-to-date with software and signatures.

Deployment Recommendations for Scanners

Instance Snapshots/Cloning Not Allowed

Using a snapshot or clone of a virtual scanner instance to create a new instance is strictly prohibited. The new instance does not functions as a scanner. All configuration settings and platform registration information will be lost. This could also lead to scans failing and errors for the original scanner.

Moving/Exporting Instance Not Allowed

Moving or exporting a registered scanner instance from a virtualization platform (HyperV, VMware, XenServer) in any file format to Microsoft Azure cloud platform is strictly prohibited. This breaks scanner functionality and the scanner permanently loses all of its settings.

Virtual machine size for hosting the scanner

To host the Qualys Virtual Scanner Appliance, maximum recommended limit by Qualys is 16 CPUs and 16 GB RAM. Based on the frequency of scanning, and the number of Azure Virtual machines that are being scanned, you can scale up to 16 CPUs and 16 GB RAM.

What do I Need?

The Virtual Scanner option must be turned on for your account. Contact Qualys Support or your Technical Account Manager if you would like us to turn on this option for you.

You must be a Manager or a sub-user with the “Manage virtual scanner appliances” permission. This permission may be granted to Unit Managers. Your subscription may be configured to allow this permission to be granted to Scanners.
Deploying Qualys Scanner Appliance

Extend the reach of the Qualys Cloud Platform to your Microsoft Azure infrastructure by deploying a Qualys Virtual Scanner Appliance - using Azure Resource Manager deployment. The appliance is a stateless resource that acts as an extension to the Qualys Cloud Platform. Once configured, all functionality is managed using your Qualys Cloud Platform account.

Here, we’ll describe how to deploy the Qualys Virtual Scanner Appliance using Microsoft Azure Resource Manager (ARM) or Resource Manager Templates. This scanner, once deployed, functions as a standard Virtual Scanner and can scan based on IP address or CIDR block.

Quick Steps

Create Resource Group in Azure
Create Storage Account in Azure
Create Virtual Network in Azure
Add New Virtual Scanner in Qualys
Scanner Configuration in Azure using Resource Manager (ARM)
Scanner Configuration in Azure using Resource Manager Templates

Create Resource Group in Azure

We recommend you create one resource group per location for your Qualys virtual scanners. Give your resource group a name that is easy to recognize and represents the group location. Once created, the name cannot be changed.

Navigate to Resource groups > Add. Provide name for the resource group, choose the subscription and location that you want to associate your resource group with. Click Create.
Create Storage Account in Azure

If you don’t already have a storage account for your Qualys virtual scanners, you’ll need to create one. Navigate to All resources > Add > Storage Account.

1) Give the storage account a name following Microsoft Azure guidelines. The name cannot be changed later.

2) Choose the deployment model “Resource manager”.

3) Choose “Use existing” for the resource group, and select the resource group you created.
Create Virtual Network in Azure

You may already have a virtual network set up for your Qualys virtual scanners. If not, create a new virtual network.

1) Give your network a name. We recommend including the location in the name so you know where the network is.

2) Choose “Use existing” for the resource group, and select the group created in the first step.

Add New Virtual Scanner in Qualys

You’ll create a virtual scanner in the Qualys Cloud Platform, assign it a distinct scanner name and record the exact personalization code.

Select VM or PC from the Qualys app picker. Then navigate to Scans > Appliances and select New > Virtual Scanner Appliance.
Choose “I have My Image” and click Continue.

Provide a name and click Next.

If you’re a sub-user then you’ll need to pick an asset group that has been assigned to your business unit by a Manager user (as shown below). Not seeing any asset groups? Please ask a Manager to assign an asset group (other than the All group) to your business unit.
Follow the on-screen instructions to configure your virtual scanner. Click Next.

Get your personalization code. You’ll need this for the configuration in Azure.

Scanner Configuration in Azure using Resource Manager (ARM)
Find and select Qualys Virtual Scanner Appliance in the Marketplace.
Review the requirements on the screen. When you’re ready to proceed, click Create to set up your virtual scanner.

Make these settings:

1) Give the virtual scanner a name. This is the name that appears in the Virtual machines list in Microsoft Azure.

Tip - Use the scanner name assigned to the virtual scanner in Qualys for easy identification.

2) The User name is your personalization code, retrieved from the Qualys platform, with a “u” prepended: “u2009XXXXXXXXXX”.

3) Choose “Use existing” for the resource group, and select the group created in the first step.
Since Qualys Virtual Scanner is a locked-down Linux appliance, managed completely from the Qualys Cloud Platform, Azure username, password and SSH public key are not used for any kind of authentication but rather as a mechanism to pass configuration information from Azure Cloud to the appliance.

- Azure passwords should not contain these special characters: `@ & < > - " ' \\
- Passwords that look like “proxy://[user:password@]IP[:port]” URLs could be used to configure Qualys Scanner to use SSL proxy for all outbound communication with the Qualys Cloud Platform.

Choose a size for your virtual scanner - up to 16 cores and no more than 16 GB. We recommend a ratio of 3-4 GB of memory per core. Other storage settings like number of data disks, max IOPS, load balancing, etc can be ignored and should not factor into your decision. For instance, the disk options does not have a significant impact on the performance of your scanner.
Be careful to choose the correct storage account and the network created in the previous steps for your Qualys virtual scanners. We do not use Azure extensions or availability sets.

Confirm your virtual scanner settings, click OK.

Review the Offer details and click Purchase. Your virtual scanner appears on the Virtual machines list in Microsoft Azure.

The Qualys Virtual Scanner Appliance appears on your Microsoft Azure Dashboard.

Your scanner updates and connect to the Qualys Cloud Platform. This process may take some time, depending on location. Once connected, you’ll be able to use your Azure scanner from the Qualys Cloud Platform as you would any virtual scanner appliance.

**Scanner Configuration in Azure using Resource Manager Templates**

Here we’ll tell you how to use Azure CLI with Resource Manager templates to deploy a Qualys Scanner in Azure.

- Your template can be a local file or an external file which is available through a URI.
Securing Microsoft Azure with Qualys
Deploying Sensors

- You must enable “Programmatic deployment” once for every new version of the Qualys Virtual Scanner Appliance Marketplace subscription.

**Step 1 - Enable Programmatic Deployment**

From the Azure UI, go to the Microsoft Azure Portal and add a new Virtual Machine. Find Qualys in the Azure Marketplace. Then click the link “Want to deploy programmatically? Get started” (see the image below). On the next screen, click “Enable” for the subscription for which you want to configure programmatic deployment and click “Save”.

**Step 2 - Deploy Your Qualys Scanner from Azure CLI**

You can download the Qualys Scanner Marketplace templates from here:

https://github.com/Qualys/azure-cloud

Edit the `azuredeploy.parameters.json` file and set all needed parameters according to your own Azure environment. Then in ARM mode use the following Azure CLI command to deploy your Qualys Scanner.

```
azure group deployment create <NameOfExistingResourceGroup> 
<NameOfQualysScanner> -f <PathToTemplate> -e <PathToParameterFile>
```

**How do I know my scanner is ready to use?**

Check your virtual scanner status in Qualys. Go to Vulnerability Management > Scans > Appliances, and find your scanner in the list.
Tip - It can take several minutes for the Qualys user interface to get updated after you add a new appliance. Refresh your browser periodically to ensure that you are seeing the most up-to-date details.

The 🟢 icon tells you your virtual scanner is ready. Now you can start internal scans!

**How to troubleshoot issues with the scanner**

Enable boot diagnostics. Diagnostics includes log output from the scanner. Set Status to On, select the storage account created for your Qualys scanners, select the Boot diagnostics check box, and hit Save (appears above the settings).
Check out these sample diagnostics.
Deploying Scanners in Private Cloud Platform

This section helps you to deploy Qualys scanner in private cloud platform using different methods.

Deploying Qualys Scanners (using CLI)

Here, we’ll describe how to deploy Qualys Virtual Scanner Appliances using “azure” or “az” CLI tools. This scanner, once deployed, functions as a standard Virtual Scanner and can scan based on IP address or CIDR block.

Want to learn more about Microsoft Azure? Check out the Azure Support page.

Quick Steps
- Creating Resource Group
- Creating Storage Account
- Creating Storage Container
- Creating Virtual Network
- Creating Deployment templates
- Copying Qualys image into your Storage Account
- Deploying Qualys Scanner

Creating Resource Group

We recommend you create one resource group per location for your Qualys virtual scanners. Give your resource group a name that is easy to recognize and represents the group location, and tell us where the group is created. Once created, the name cannot be changed.

azure CLI

Example: azure group create --name resource-group-qualys-scanner --location "Central US"

az CLI

Example: az group create --name resource-group-qualys-scanner --location centralus

where name is the resource group name, and location is the location where we create the group

Help: -h, --help for output usage information

Creating Storage Account

We recommend you create at least one storage account for your Qualys virtual scanners.

azure CLI

Example: azure storage account create storagequalys --resource-group
resource-group-qualys-scanner --sku-name LRS --kind Storage --location "Central US"

az CLI
Example: az storage account create --name storagequalys --resource-group resource-group-qualys-scanner --sku Standard_LRS --kind Storage --location centralus

where name is the storage account name, resource-group is the resource group name, sku is the SKU name (Premium_LRS, Standard_GRS, Standard_LRS, Standard_RAGRS, Standard_ZRS), kind is the account kind (BlobStorage, Storage, StorageV2), location is the location

Help: -h, --help for output usage information

Creating Storage Container
You need to create a container in your storage account where qvsa images are stored.

azure CLI
Example: azure storage container create --container images --account-name storagequalys --account-key "AbcdefDKBFEHMKxee1zL4fsxIN1m7gPrG+dVoirJFvCVEknW9TbCXVEUDxs1Oeg+heAcosc /SiCUhAzwN0uy+2w=="

az CLI
Example: az storage container create --name images --account-name storagequalys --account-key "AbcdefDKBFEHMKxee1zL4fsxIN1m7gPrG+dVoirJFvCVEknW9TbCXVEUDxs1Oeg+heAcosc /SiCUhAzwN0uy+2w=="

where name is the storage container name, account-name is the storage account name, account-key is the storage account key

Help: -h, --help for output usage information

Creating Virtual Network
You may already have a virtual network set up for your Qualys virtual scanners. If not, create a new virtual network with 10.0.0.0/24 subnet.

azure CLI
Example: azure network vnet create --name qualys-scanner-vnet --address-prefixes "10.0.0.0/24" --resource-group resource-group-qualys-scanner --location "Central US"

az CLI
Example: az network vnet create --name qualys-scanner-vnet --address-prefixes "10.0.0.0/24" --resource-group resource-group-qualys-scanner --location centralus

where name is the name of the virtual network, address-prefixes is a comma separated list of address prefixes for this virtual network, resource-group is the name of the resource group, location is the location.

Help: -h, --help for output usage information

Creating Deployment templates
To deploy Qualys scanner from the command line you need to create deployment templates.

Microsoft Documentation on Azure Resource Manager Templates
Download custom Qualys Scanner templates and adjust them to your Azure Cloud environment.

Copying Qualys image into your Storage Account
Now you need to copy Qualys qVSA image to your storage account. The qVSA image link is provided to you by Qualys Operations.

azure CLI
Example: azure storage blob copy start --source-uri "https://qvsacq5itlevnuiuku.blob.core.windows.net/images/qVSA.i386-2.4.26-2.vhd?st=2018-02-07T01%3A20%3A01Z&se=2019-02-09T01%3A20%3A01Z&sp=r1&sv=2015-02-21&sr=c&sig=vEzX1Ky6cy3Dg2Y%2F07qXVsY%3D" --account-name "storagequalys" --account-key "AbcdefDKBFEHMKxeelzL4fsxINIm7gPrG+dvOirJFDuCVEnkW9TbcXVcUEDxs1Oeg+heAcosc/SiCUHaxwN0uy+2w==" --dest-blob "qualys-scanner-image" --dest-container images

az CLI
Example: az storage blob copy start --source-uri "https://qvsacq5itlevnuiuku.blob.core.windows.net/images/qVSA.i386-2.4.26-2.vhd?st=2018-02-07T01%3A20%3A01Z&se=2019-02-09T01%3A20%3A01Z&sp=r1&sv=2015-02-21&sr=c&sig=vEzX1Ky6cy3Dg2Y%2F07qXVsY%3D" --account-name "storagequalys" --account-key "AbcdefDKBFEHMKxeelzL4fsxINIm7gPrG+dvOirJFDuCVEnkW9TbcXVcUEDxs1Oeg+heAcosc/SiCUHaxwN0uy+2w==" --destination-blob "qualys-scanner-image" --destination-container images

where source-uri is the qVSA image link provided by Qualys Operations, account-name is the storage account name, account-key is the storage account key, destination-blob is the blob name, destination-container is the destination storage container name
Help: -h, --help for output usage information

Deploying Qualys Scanner

Prior to deploying the Qualys Virtual Scanner in Azure, you must first create a virtual scanner in the Qualys Cloud Platform, assign it a distinct scanner name and record the exact personalization code.

Notes:

1) Since Qualys Virtual Scanner is a locked-down Linux appliance, managed completely from the Qualys Cloud Platform, Azure username, password and SSH public key are not used for any kind of authentication but rather as a mechanism to pass configuration information from Azure Cloud to the appliance.

2) Azure passwords should not contain these special characters: : @ & < > - " '\

3) Passwords that look like "proxy://[user:password@]IP[:port]" URLs could be used to configure Qualys Scanner to use SSL proxy for all outbound communication with the Qualys Cloud Platform.

azure CLI

Example: azure group deployment create --resource-group resource-group-qualys-scanner --name qualys-scanner --template-file azuredeploy.json --parameters-file azuredeploy.parameters.json

az CLI

Example: az group deployment create --resource-group resource-group-qualys-scanner --name qualys-scanner --template-file azuredeploy.json --parameters-file @azuredeploy.parameters.json

where resource-group is the name of the resource group, name is the name of the deployment, template-file is the path to the template file in the file system, parameters is a file containing parameters

Help: -h, --help for output usage information
Using Azure GUI to Create Qualys Image from VHD file (Optional)

You can create the Qualys image from a VHD file using the Azure GUI. You can also do this using the “azure” or “az” CLI tools (Refer to Copying Qualys image into your Storage Account).

From the Microsoft Azure Dashboard, choose Create a resource, search for images, and then click Create.

Fill in all the required information for your new image. In Storage blob, choose the location of the .vhd file you have already copied into your Storage account.
You can create one instance of a Qualys scanner using the image created in the previous step. Choose All services, then choose Images from the Compute section. Find your image in the list and Click Create VM.
Deploying Qualys Cloud Agent

This section helps you to deploy Qualys cloud agent using different methods.

Deploy Qualys Cloud Agent from Azure Security Center

This section describes how to install Qualys Cloud Agents (Windows and Linux) for Azure virtual machines from the Azure Security Center console and view vulnerability assessment findings within Azure Security Center and your Qualys subscription.

Azure Security Center provides a unified security management and monitoring console for Azure infrastructure. Qualys is integrated into the Azure security center’s partner solutions for Vulnerability assessment. The security center detects the virtual machines without the solution and automates the deployment of the lightweight Qualys cloud agents on them. The agents gather vulnerability data and send it to the Qualys Cloud Platform, which in turn, provides vulnerability and health monitoring data back to Azure Security Center.

Using our revolutionary Qualys Cloud Agent platform you can deploy lightweight cloud agents to continuously assess your infrastructure for security and compliance.

We recommend these resources

- Qualys Cloud Platform
- Qualys Cloud Agent Getting Started Guide

Quick Steps

Create Asset Tag in AssetView (Optional)
Create Activation Key in Cloud Agent
Deploy Cloud Agents in Azure

Create Asset Tag in AssetView (Optional)

Asset tags provide the ability to uniquely list out assets. As a best practice, we recommend you create a tag called “Azure” that you’ll use to easily distinguish the assets in the Azure cloud from the rest. You’ll associate the tag with the activation key in the next step.

Choose AssetView from the module picker, then go to Assets > Tags and click New Tag.

In the Tag Creation wizard, give your tag a name, and choose No Dynamic Rule under Tag Rule (required when adding tags to keys). Click Finish when you’re done.
Create Activation Key in Cloud Agent

Now we’ll describe how to create an activation key. At the end of this step you’ll have the license code and public key needed to deploy agents in Azure. We recommend you handle the Azure cloud deployments via a designated activation key. Additionally, manage your departments with separate activation keys.

Choose Cloud Agent from the module picker, then go to Agent Management > Agents and click Install New Agent.

Give the key a unique name (example: AzureAgentsActivationKey) and select VM and/or PC modules, depending on your licenses. We encourage you to have both solutions to secure your assets in Azure completely.

Did you create an asset tag for Azure? Select the tag at this time. Then click Generate.
As part of this integrated deployment, the Azure agent is currently supported for Windows and Linux. (Linux agent support is recently added).

Click the Install Instructions button for Windows or Linux.

Choose “Deploying in Azure Cloud” and retrieve the keys from the page.

Copy the License Code and Public Key. You’ll need these in the next step when you deploy cloud agents in Azure.
Deploy Cloud Agents in Azure

There are two offerings available for Azure Security Center integrations and each will be covered below:

- Vulnerability Assessment with Qualys Cloud Agent (QCA) (Bring Your Own License (BYOL))
- Azure Security Center Embedded Vulnerability Assessment Powered by Qualys

Vulnerability Assessment with Qualys Cloud Agent

Vulnerability Assessment with Qualys Cloud Agent (QCA) (Bring Your Own License (BYOL)) provides a way to deploy QCA via Azure Security Center (ASC). It also provides Auto-deploy of agents for the initially configured Azure Resource Group. This offering is available with both the free and standard tiers of ASC.

1) Login into the Microsoft Azure portal and navigate to “Security Center”. Azure Security Center integrates with Azure services to monitor and protect your Windows and Linux virtual machines.

2) Click on “Recommendations”, then click “Vulnerability assessment solution should be installed on your virtual machines”. Qualys agents are integrated into the Recommendations for the vulnerability assessment solution within the security center. Security center automatically detects the virtual machines and with this integration, users can directly deploy the Qualys Cloud Agent.
3) From the list of recommendations select one or many* virtual machines where you want to deploy the Cloud Agents. Once VMs are selected, click “Install on #n VMs” to proceed with the agent installation (Where is #n the number of virtual machines).

![Image of TAM-Demo-VM-05](Image)

4) Select 'Create New' to create a new solution. If you have already gone through the flow once, the Qualys solution is available in the “Use existing solution” list under this option.

![Image of Add a Vulnerability Assessment](Image)

5) Select “Qualys, Inc” as a vulnerability assessment solution form a list of solutions when creating a new solution.

![Image of Create a new Vulnerability Assessment solution](Image)
6) Specify configuration details for a New solution. Specify a name for the solution. Select resource group, location. Specify License code and Public key for solution. You can get License code and Public key from Activation key you created in your Qualys subscription.

7) Optionally, you can specify to enable the “Auto deploy” option. This option is specific to ASC Vulnerability assessment and not associated with specific third-party applications such as Qualys, etc. When the “Auto deploy” option is On, it deploys Qualys Cloud Agent automatically on VMs. These VMs are provisioned recently in Resource Group which was specified while creating the solution. For example, the Resource group mentioned in the above screen shot have if the Auto deploy option is enabled, Qualys agent gets automatically deploys for newly provisioned VMs only in Resource group “AutoDeployEU”.
8) You need to have a subscription with Qualys to get the license code and public key needed for deploying the agent. When generating the Agent key toggle the “Deploying in Azure Cloud” selector.
9) Follow the section inline, to retrieve the License code and Public Key. If you are NEW to Qualys, you can review the Qualys solution and sign up for a free trial from 'Sign up for the solution' link.

Note: For subsequent deployments, choose the solution you just created from the 'Existing Solution' list. The inputs are saved, so you don’t need to retrieve the code and key from your Qualys subscription again.

**Retrieve the License Code and Public Key from your Qualys Subscription**

1) Login to your Qualys subscription. Navigate to the “Cloud Agent” application from the menu, then select “Activation Keys”.
2) Click “New Key” and generate a new activation key. We recommend you handle the Azure cloud deployments via a separate Activation Key. Additionally, manage your departments with separate activation keys. Specify a name to identify it uniquely (example: Azure Security Center Key) and select Vulnerability Management and/or Policy compliance modules depending on your licenses. We encourage you to have both the solutions to secure your assets in Azure completely.
3) Specify a name to identify it uniquely (example: Azure Security Center Key) and select Vulnerability Management and/or Policy compliance modules depending on your licenses. We encourage you to have both the solutions to secure your assets in Azure completely. Click Generate for new activation key.

4) Currently, as a part of this integrated deployment is only available for Windows and Linux agents. (Linux agent support is newly added). Click 'Install Instructions' under Windows or Linux. Choose 'Deploying on Azure' and retrieve the keys from the page.
5) Copy the License code and Public key and use it in during Deploying the agent.

Azure Security Center Embedded Vulnerability Assessment Powered by Qualys

Azure Security Center Embedded Vulnerability Assessment Powered by Qualys helps to quickly deploy a Vulnerability Assessment Solution powered by Qualys. No other configurations needed. This offering is available to all Azure customers that are subscribed to the Azure Security Center (ASC) standard pricing tier.

This solution utilizes the Qualys Cloud Agent that will be deployed to your virtual machines in your Azure subscription. The Vulnerability Assessment findings will be populated into your ASC Dashboard under recommendations.

1) Login into the Microsoft Azure portal and navigate to “Security Center”. Azure Security Center integrates with Azure services to monitor and protect your Windows and Linux virtual machines.

2) Click on “Recommendations”, then click “Enable the built-in vulnerability assessment solution on virtual machines (powered by Qualys)”.

![Azure Security Center Embedded Vulnerability Assessment Powered by Qualys](image-url)
Embedding Qualys Cloud Agent as a part of Golden Machine Image

The Qualys Cloud Agent supports configuration and deployment into cloned images in cloud environments such as Microsoft Azure. For step-by-step procedure, kindly contact your TAM or Qualys Support for “Cloud Agent Technical White Paper”.

Deploy Qualys Cloud Agent via Azure ARM Template

This section helps you to deploy Qualys Cloud Agent using Azure Resource Manager (ARM) template.

Using Azure Portal

Deploy Cloud Agent on Linux VM

Deploy Cloud Agent on Windows VM

Using Powershell

```
PS C:\> New-AzureRmResourceGroupDeployment -VMName VM_NAME -ResourceGroupName RESOURCE_GROUP_NAME -Location VM_LOCATION -TemplateFile TEMPLATE_FILE_PATH -TemplateParameterFile TEMPLATE_PARAMETER_FILE_PATH
```

where,

- TEMPLATE_FILE_PATH = the path of the template file
- TEMPLATE_PARAMETER_FILE_PATH = the path of parameter file for the template

Input Parameters: utilize azuredeploy-parameters.json as an example to supply parameters field.

- vmName: The name of the Virtual Machine where you want to install Qualys Cloud Agent
- vmlocation: The location of the Virtual Machine
- LicenseCode: The License Code from your Qualys Subscription

Deploy Qualys Cloud Agent via Other Tool Sets

Qualys Cloud Agent can be deployed via automation, orchestration or configuration management tools sets in your environment, for example, Ansible, Chef, and Puppet. Qualys provides a template for deploying Qualys Cloud Agent via Ansible. This can be used by customers to deploy and configure Qualys Cloud Agent in their Azure environment.

Ansible

This section helps you to deploy Qualys Cloud Agent using Ansible-Playbook.

The playbook InstallQCA.yml can be used to deploy Qualys Cloud Agent across the assets included in your “host” file. Additionally, you can use the tags to deploy Qualys Cloud Agent on your virtual machines. Refer Cloud Agent Ansible for github example.

The required input parameters are:
- private-key = private-key to access the virtual machines (Ansible works via SSH)
- ssh_user = username to login into the instance
- URL = the URL where the file is hosted For example: Webserver, S3, Blob Storage, Cloud Storage
- ActivationID = An ID that provides a way to group agents and bind them to your account
- CustomerID = An ID to identify your account

**Azure Automation Cloud Agent**

This section help you to deploy Qualys Cloud Agent in Azure Virtual Machine (VM) using Azure Automation and Run command.

The powershell script “qcainstall.ps1” logs into the Azure subscription and locates all the Resource Groups in it. Crawling each Resource Groups, it locates VMs inside them. With the help of Azure Run command ”Invoke-AzureRmVMRunCommand”, it downloads the script to install Qualys Cloud Agent based on Operating System (OS) of the VM.

Pre-requisites: You should have an Azure automation account and an Automation connection asset named ”AzureRunAsConnection” in that Azure automation account.

Note: This script only works on powershell version 2 and above. It specifically not works for V5 core due to unavailability of Invoke-webrequest cmdlet. You can opt for the alternatives.

**Usage:**

1) Create variables named ContainerName, StorageAccountName, StorageAccountKey.
2) Copy the executables files (Qualys Cloud Agent exe, rpm or deb files) and upload it to the Blob storage that is publicly accessible.

3) Repeat the steps 1 and 2 for scripts LinucQCA.sh and WindowsQCA.ps1 and store it in Blob storage referred by variables created in step 1 and let it be private.

4) Import the main script named qcainstall.ps1 into Azure automation runbook and edit the variables and Save and publish it. ActivationId, CustomerId, url_rpm, url_deb.
5) Start the Runbook.
Scan Assets

This section helps to understand the steps to scan your network. Before you initiate your scan, you must ensure few check points/pre-configurations.

Azure Scan Checklist

We recommend these steps before scanning.

- Check Appliance Status
- Configure OS Authentication
- Configure security groups for the Azure virtual machines to be scanned

Check Appliance Status

Go to Scans > Appliances - Be sure the new Scanner Appliance is connected to the Qualys Cloud Platform. 🟢 means your appliance is connected and ready for scanning.
Configure OS Authentication

Using host OS authentication (trusted scanning) allows our service to log in to each target system during scanning. Running authenticated scans gives you the most accurate results with fewer false positives.

Go to Scans > Option Profiles. Edit the profile Initial Options, use Save As to save a copy with another name. In your new profile enable the authentication types you’ll need.

Go to Scans > Authentication. Add authentication records for the Azure virtual machines you’ll be scanning - Unix and/or Windows. In the record you’ll need to add credentials for the account to be used for authentication - this is an account for OS user (not the AIM user). We recommend you create a dedicated account for authentication on target systems.
Sample Unix Record

1) Login Credentials - Provide OS user name and select Skip Password.

2) Private Keys - Key authentication recommended. Select key type (RSA, DSA, ECDSA, ED25519) and enter your private key content.
3) IPs - Select Unix IP addresses/ranges of your Azure virtual machines for this record. Credentials in this record are used to scan these assets.

Sample Windows Record
1) Login Credentials - Provide OS user name and select Skip Password.
2) IPs - Select Windows IP addresses/ranges of your Azure virtual machines for this record. Credentials in this record are used to scan these assets.

Learn more about OS authentication
Online help within the authentication record workflows provides detailed instructions and guidance on all available options. These documents are good resources

Qualys Windows Authentication Guide (pdf)
Qualys Unix Authentication Guide (pdf)
Configure security groups for the Azure virtual machines to be scanned
In Azure, you must associate a security group that allows inbound access on all ports for the IP address of the scanner appliance or the security group of the scanner appliance.

Tips and Best Practices

Have Qualys Defined Networks? Move your Virtual Appliance
This step is recommended if you’ve defined custom networks in your Qualys account.

By default a new Virtual Scanner Appliance is placed in the Global Default Network and when a scan is performed, host scan data is added to that network. We recommend you move this Virtual Appliance to the desired network before scanning a custom network.

Go to Assets > Networks, edit the network you want to move the Virtual Appliance to and add the appliance to that network.

Internal Scanning using Virtual Scanner Appliance
Scanning with pre-authorized scanner appliance involves following sequence of steps.

1) Create a dynamic tag with Cloud Asset Search filters under “AssetView” app based on your requirements.
   For example:
   All running VMs in your Qualys Subscription: `azure.vm.state:"RUNNING"`
   All running VMs in your Azure Subscription: `azure.vm.subscriptionId:<your Azure Subscription Id> and azure.vm.state:"RUNNING"`
   All running VMs in a location: `azure.vm.state:"RUNNING" and azure.vm.location:westus`
   All running VMs in a resource group: `azure.vm.state:"RUNNING" and azure.vm.resourceGroupName:testRG`

2) Extract IP addresses of machines returned by tags created in above step. You can extract it using Download or API Query to Host Assets.

3) Add these IP addresses grouped as Asset Groups or individually as Host Assets under Assets tab in Vulnerability Management.

4) Configure OS Authentication records.

5) Now, lets start scanning. Go to Scans > Scans > New > Scan (or Schedule Scan).
6) Identify your scan target. Click Assets to select a combination of asset groups and IP addresses to scan or click Tags to select one or more asset tags to scan.
7) That’s it - just click Launch and you're done!
Internal Network Scanning using Qualys Cloud Agent

Using our revolutionary Qualys Cloud Agent platform you can deploy lightweight cloud agents to continuously assess your Azure infrastructure for security and compliance.

Cloud Agent features
- Communicates to the Qualys Cloud Platform over port 443 and supports Proxy configurations.
- Supports scanning a range of Linux and Windows OS versions

Get Started
Navigate to the Cloud Agent (CA) app and install the Cloud Agent in minutes

Perimeter Scanning using Qualys External Scanners

Qualys External Scanners (Internet Remote Scanners), located at the Qualys Cloud Platform are used for Perimeter Scanning of Azure virtual machines.
- You’ll use the Standard Scan workflow in Qualys.
- Customers need to add the Public IPs of the virtual machines to your account.
- Qualys External Scanners support both IP-based scans and DNS-based scans.
Get Started

1) Create a dynamic tag with Cloud Asset Search filters under “AssetView” app based on your requirements.

For example:

All running public VMs in your Qualys Subscription: `not azure.vm.publicIpAddress is null and azure.vm.state:"RUNNING"`

All running public VMs in your Azure Subscription: `not azure.vm.publicIpAddress is null and azure.vm.subscriptionId: and azure.vm.state:"RUNNING"`

All running public VMs in a location: `not azure.vm.publicIpAddress is null and azure.vm.state:"RUNNING" and azure.vm.location:westus`

All running public VMs in a resource group: `not azure.vm.publicIpAddress is null and azure.vm.state:"RUNNING" and azure.vm.resourceGroupName:testRG`

2) Extract IP addresses of machines returned by tags created in above step. You can extract it using Download or API Query to Host Assets.

3) Add these IP addresses grouped as Asset Groups or individually as Host Assets under Assets tab in Vulnerability Management.

4) Now, lets start scanning. Go to Scans > Scans > New > Scan (or Schedule Scan).

5) Identify your scan target. Click Assets to select a combination of asset groups and IP addresses to scan or click Tags to select one or more asset tags to scan. For Option Profile, we recommend Initial Options to get started; for Scanner Appliance select the External option; for scan target choose IP addresses/asset groups or asset tags defined using Qualys AssetView (AV).
6) That’s it - just click Launch and you’re done!

**Scan option profile settings**

As a part of the scan option profile, the scanner tries to reach out the IPs and try to get to the virtual machines. Ensure that you enable authentication for Windows and/or Unix. See [Configure OS Authentication](#).
Cloud Inventory and Security Assessment

This section describes about discovery of cloud inventory such as cloud assets and resources. It also describes about security assessment giving full visibility into the public cloud security posture of all assets and resources.

Cloud Inventory

Qualys Cloud Inventory continuously discovers and tracks assets and resources such as virtual machines, SQL databases, Network security groups, WebApps and others, across all regions and multiple subscriptions in Microsoft Azure and gives you an “at-a-glance” comprehensive picture of your cloud inventory and the location of assets across global regions. You can view all this information in one central place.

Features:

- Provides a quick overview of inventory via pre-built dashboards, and lets you personalize or build your own with custom widgets
- Collects rich metadata for every resource and shows associations across resources, so you can understand scenarios such as what security groups are potentially public and unprotected, and which related assets this is impacting
Cloud Security Assessment

Qualys Cloud Security Assessment gives full visibility into the public cloud security posture of all assets and resources. Refer to CloudView Getting Started Guide for more details.

Features:

- Provides a quick overview of inventory and security posture via dashboards
- Lets you personalize or build your own with custom widgets based on queries or on other criteria, such as “Top 10 accounts based on failures” and “Top 10 controls that are failing”
- Out of box Azure policies like CIS Microsoft Azure Foundations Benchmark and Azure Best Practices Policy
- Continuously assess and report on resource mis-configurations by checking against the controls from out-of-box policies
- Build your own policies and customize controls to suit your need
- Ability to view, filter and export mis-configurations
Securing Web Applications

Using Qualys you can secure Applications using Application Scanning and Firewall solutions.

Qualys WAS

Qualys Web Application Scanning (WAS) provides automated crawling and testing of custom web applications to identify application and RESTAPI vulnerabilities including cross site scripting (XSS) and SQL injection. To get started install the Qualys Virtual Scanner Appliance that’s pre-authorized by Azure. This is the same appliance used to scan for vulnerabilities and compliance checks.

How do I get started?
- Follow the steps in Deploying Qualys Scanner
- Then review instructions in Qualys Web Application Scanning Getting Started Guide.

Qualys WAF

Protect applications with firewall rules and instant virtual patches using Qualys Web Application Firewall (WAF).

How do I get started?
- Install the Web Application Firewall Appliance available on the Azure
- Then review instructions in Qualys Web Application Firewall Getting Started Guide.
Securing Containers

Qualys Container Security provides discovery, tracking and continuously protecting container environments. This addresses vulnerability management for images and containers in their DevOps pipeline and deployments across cloud and on-premise environments.

Qualys Container Security supports:
- Discovery, inventory and near-real time tracking of container environments
- Vulnerability analysis for images and containers
- Vulnerability analysis for registries
- Integration with CI/CD pipeline using Jenkins/Bamboo Plugins or REST APIs (DevOps flow)

Refer Qualys Container Security User Guide for more details.
Deploying Container Sensor

The sensor from Qualys is designed for native support of Docker environments. Sensor is packaged and delivered as a Docker Image. Download the image and deploy it as a Container alongside with other application containers on the host.

Since they are docker based, the sensor can be deployed into orchestration tool environments like Kubernetes, Mesos or Docker Swarm just like any other application container.

Refer Qualys Container Security Deployment Guide for more details.
Analyze, Report & Remediate

This section covers - how to query assets, build widgets and dashboards, and then how to generate vulnerability reports on Azure assets.

How to Query Azure Assets

Our advanced search capabilities help you to quickly find all about your assets all in one place. Choose the AssetView app and go to the Assets tab. This is where you’ll see an inventory of all your scanned assets. Say you want to find all your Azure assets. Type provider and select Azure from the drop-down menu.

You can search many Azure asset properties. Start typing Azure and you’ll see a list Azure asset properties (tokens) you can use to search. Hover over the token name to see syntax help to the right.
View Asset Details Anytime

The latest vulnerability and compliance data is always available in your assets inventory. Just select the asset name and choose View Asset Details from the quick actions menu.

Save Query

Easily save your searches for reuse and share them with other users.
Download and Export Results

It just takes a minute to export search results. Select Download from the Tools menu. Next choose an export format and click Download - choose from multiple formats.

Create Widget

You can create a widget based on your query and add it to your dashboard. For example, first search for Azure assets that have not been scanned for vulnerabilities using Qualys VM for a month. Here’s your query:

provider:"Azure" AND NOT lastVmScanDate: [now-30d..now-1s]

Then choose Create widget. Add a title, you’ll see your query is populated for you, just one click to add to your dashboard.
Creating Reports

You can create many different reports on vulnerabilities in the Qualys VM app.

Go to Reports > New > Scan Report > Template Based. There are many report templates to choose from, or you can create your own. Try the Technical Report to see full vulnerability details in your report.

Want to report on compliance data? No problem. Choose PC from the module picker. Then go to Reports > New > Compliance Report, and pick the report you’re interested in.
Dynamic Tagging Using Azure Attributes

Create dynamic tag rules to tag your Azure virtual machines based on Azure metadata as collected by the Azure Connector. For each tag rule you’ll provide a search query with Azure instance information.

It’s easy to get started! 1) Click New Tag, 2) choose the Cloud Asset Search tag rule, 3) select the cloud provider, and 4) enter your query. Just start typing in the Query field and we’ll show you the Azure attributes you can search.

Sample queries

Find Azure virtual machines located in East US region: azure.vm.location: eastus

Find Azure virtual machines with specific group name: azure.vm.resourceGroupName: MC_hkkube_hkaks2_eastus

Find Azure virtual machines of standard size: azure.vm.size: Standard*

Find Azure virtual machines based on IPs (comma-separated list or range): azure.vm.publicIpAddress: [104.211.13.0 ... 104.211.13.255] azure.vm.privateIpAddress: [10.95.0.0... 10.95.0.255]

Find Azure virtual machines for specific subscription ID: azure.vm.subscriptionId: 1d767489-da0c-4948-a285-bf2c708c0586

Find Azure virtual machines for specific tags: azure.tags: (name: owner and value: amy)
Manage Assets Using Qualys

Here’s some best practices and tips for organizing assets to help you secure Azure infrastructure using Qualys.

Setting up Qualys Configurations

**Asset Groups** - Organize assets into meaningful groups and assign them to sub-users. Asset groups are required when you have multiple users i.e. Scanner, Reader, Unit Manager (if business units are defined). The same IP address can be included in multiple asset groups.

![Asset Groups screenshot]

**Business Units** - Organize users and assets into business units in a way that matches your organization. This gives Managers the ability to grant users role-based permissions in the context of their assigned business unit. The same IP address can be included in multiple business units.

![Business Units screenshot]

**Networks** - Organize discrete private IP networks to keep overlapping IP blocks separate. When configured Qualys tracks IPs by network and IP address. Keep in mind... An IP address must be unique to your subscription or a single network.

![Networks screenshot]
Removing Terminated Virtual Machines - You can remove terminated virtual machines from your Qualys account. Go to Vulnerability Management or Policy Compliance > Assets > Asset Search and select the assets with tracking method as IP address. You could also add more parameters to refine your such as Last Scan Data not within x days and so on.
Click Search and then select the assets from the results. From the Actions drop-down, select Purge. This results in removal of assets along with their associated data from the module.

Uninstall agents

Consider a scenario where you have deployed cloud agents on your Azure assets and you want to uninstall agents not checked-in for last N days, you can use the API call.

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

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

For more information on Cloud Agent APIs, refer to our Cloud Agent API User Guide.
## Common Questions

<table>
<thead>
<tr>
<th>Queries</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>How to view platform provider info on virtual scanner appliances?</td>
<td>You’ll see the platform provider info for a virtual scanner appliance that’s been deployed in Azure (or another cloud platform) within your Qualys account. You’ll see this info in the General Information section when you view or edit the appliance (from Scans &gt; Appliances).</td>
</tr>
<tr>
<td>Troubleshooting connectivity</td>
<td>Qualys Scanner Appliance must make regular connections to the Qualys Cloud Platform over HTTPS. Please be sure to resolve connectivity issues to ensure proper functioning of your appliance.</td>
</tr>
<tr>
<td></td>
<td>The Communication Failure message appears if there is a network breakdown between the scanner and the Qualys Cloud Platform. The communication failure may be due to one of these reasons: the local network goes down, Internet connectivity is lost for some reason, or any of the network devices between the scanner and the Qualys Cloud Platform goes down.</td>
</tr>
<tr>
<td></td>
<td>The Network Error message indicates the Scanner Appliance attempted to connect to the Qualys Cloud Platform and failed. You’ll see an error code and description to help you with troubleshooting. Errors can be related to the proxy server and connection errors with Qualys Cloud Platform. The Qualys Cloud Platform logs results of connectivity checks and overall personalization process on the Azure System Console.</td>
</tr>
<tr>
<td></td>
<td>If you see “No connectivity to qualysguard.qualys.com - please fix.” messages, please verify that your VPN Network ACLs and Security Groups allow outbound HTTPS (TCP port 443) access. If you are using a proxy server, ensure that the scanner can reach the proxy server, and that the proxy server can access the Qualys cloud platform.</td>
</tr>
</tbody>
</table>